EXHIBIT A

Supreme Court of Pennsylvania

Court of Common Pleas
Civil Cover Sheet

Cambria County

For Prothonotary Use Only:	Prothonotary Cambria Co, PA. FILED
Docket No: 2023-1430	APR 18 '23 PM 12:19

The information collected on this form is used solely for court administration purposes. This form does not supplement or replace the filing and service of pleadings or other papers as required by law or rules of court.

SECTION A

Commencement of Action:
☒ Complaint ☐ Writ of Summons ☐ Petition
☐ Transfer from Another Jurisdiction ☐ Declaration of Taking

Lead Plaintiff's Name:	Lead Defendant's Name:
Jane Doe	DLP CONEMAUGH MEMORIAL MEDICAL CENTER, LL
Are money damages requested? ☒ Yes ☐ No	Dollar Amount Requested: (check one) ☐ within arbitration limits ☒ outside arbitration limits
Is this a *Class Action Suit*? ☒ Yes ☐ No	**Is this an *MDJ Appeal*?** ☐ Yes ☒ No

Name of Plaintiff/Appellant's Attorney: Elizabeth Bailey Esq., Saltz Mongeluzzi, et al.

☐ **Check here if you have no attorney (are a Self-Represented [Pro Se] Litigant)**

SECTION B

Nature of the Case: Place an "X" to the left of the **ONE** case category that most accurately describes your ***PRIMARY CASE***. If you are making more than one type of claim, check the one that you consider most important.

TORT *(do not include Mass Tort)*
- ☐ Intentional
- ☐ Malicious Prosecution
- ☐ Motor Vehicle
- ☐ Nuisance
- ☐ Premises Liability
- ☐ Product Liability *(does not include mass tort)*
- ☐ Slander/Libel/ Defamation
- ☒ Other: Intrusion upon Seclusion

MASS TORT
- ☐ Asbestos
- ☐ Tobacco
- ☐ Toxic Tort - DES
- ☐ Toxic Tort - Implant
- ☐ Toxic Waste
- ☐ Other:

PROFESSIONAL LIABLITY
- ☐ Dental
- ☐ Legal
- ☐ Medical
- ☐ Other Professional:

CONTRACT *(do not include Judgments)*
- ☐ Buyer Plaintiff
- ☐ Debt Collection: Credit Card
- ☐ Debt Collection: Other
- ☐ Employment Dispute: Discrimination
- ☐ Employment Dispute: Other
- ☐ Other:

REAL PROPERTY
- ☐ Ejectment
- ☐ Eminent Domain/Condemnation
- ☐ Ground Rent
- ☐ Landlord/Tenant Dispute
- ☐ Mortgage Foreclosure: Residential
- ☐ Mortgage Foreclosure: Commercial
- ☐ Partition
- ☐ Quiet Title
- ☐ Other:

CIVIL APPEALS
Administrative Agencies
- ☐ Board of Assessment
- ☐ Board of Elections
- ☐ Dept. of Transportation
- ☐ Statutory Appeal: Other
- ☐ Zoning Board
- ☐ Other:

MISCELLANEOUS
- ☐ Common Law/Statutory Arbitration
- ☐ Declaratory Judgment
- ☐ Mandamus
- ☐ Non-Domestic Relations Restraining Order
- ☐ Quo Warranto
- ☐ Replevin
- ☐ Other:

Updated1/1/2011

NOTICE

Pennsylvania Rule of Civil Procedure 205.5. (Cover Sheet) provides, in part:

Rule 205.5. Cover Sheet

(a)(1) This rule shall apply to all actions governed by the rules of civil procedure except the following:

(i) actions pursuant to the Protection from Abuse Act, Rules 1901 et seq.

(ii) actions for support, Rules 1910.1 et seq.

(iii) actions for custody, partial custody and visitation of minor children, Rules 1915.1 et seq.

(iv) actions for divorce or annulment of marriage, Rules 1920.1 et seq.

(v) actions in domestic relations generally, including paternity actions, Rules 1930.1 et seq.

(vi) voluntary mediation in custody actions, Rules 1940.1 et seq.

(2) At the commencement of any action, the party initiating the action shall complete the cover sheet set forth in subdivision (e) and file it with the prothonotary.

(b) The prothonotary shall not accept a filing commencing an action without a completed cover sheet.

(c) The prothonotary shall assist a party appearing pro se in the completion of the form.

(d) A judicial district which has implemented an electronic filing system pursuant to Rule 205.4 and has promulgated those procedures pursuant to Rule 239.9 shall be exempt from the provisions of this rule.

(e) The Court Administrator of Pennsylvania, in conjunction with the Civil Procedural Rules Committee, shall design and publish the cover sheet. The latest version of the form shall be published on the website of the Administrative Office of Pennsylvania Courts at www.pacourts.us.

SALTZ MONGELUZZI & BENDESKY P.C.
BY: ELIZABETH A. BAILEY
ONE LIBERTY PLACE, 52ND FLOOR
1650 MARKET STREET
PHILADELPHIA, PA 19103
(215) 496-8282

COHEN & MALAD, LLP
BY: LYNN TOOPS/AMINA A. THOMAS
PRO HAC VICE PENDING
ONE INDIANA SQUARE, SUITE 1400
INDIANAPOLIS, IN 46204
(317) 636-6481

TURKE & STRAUSS LLP
BY: RAINA C. BORRELLI/SAMUEL J. STRAUSS
PRO HAC VICE PENDING
613 WILLIAMSON STREET, SUITE 201
MADISON, WI 53703
(608) 237-1775

STRANCH, JENNINGS & GARVEY, PLLC
J. GERARD STRANCH, IV/ANDREW E. MIZE
PRO HAC VICE PENDING
223 ROSA L. PARKS AVENUE, SUITE 200
NASHVILLE, TN 37203
(615) 254-8801

Attorneys for Plaintiff

CAMBRIA COUNTY COURT OF COMMON PLEAS

JANE DOE Individually, and on behalf of all others similarly situated,	Case No. 2023-1430
Plaintiff	
v.	JURY TRIAL DEMANDED
DLP CONEMAUGH MEMORIAL MEDICAL CENTER, LLC D/B/A CONEMAUGH HEALTH SYSTEM D/B/A CONEMAUGH MEMORIAL MEDICAL CENTER	

1086 Franklin Street
Johnstown, Pennsylvania 15905

-and-

DLP CONEMAUGH PHYSICIAN PRACTICES, LLC D/B/A CONEMAUGH PHYSICIAN GROUP - OB/GYN
1111 Franklin Street
Suite 300
Johnstown, Pennsylvania 15905

Defendants

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff, JANE DOE, Individually, and on behalf of all others similarly situated (hereinafter "Plaintiff") brings this Class Action Complaint against the Defendants, DLP CONEMAUGH MEMORIAL MEDICAL CENTER, LLC, d/b/a Conemaugh Health System d/b/a Conemaugh Memorial Medical Center ("Conemaugh Health System"), and DLP CONEMAUGH PHYSICIAN PRACTICES, LLC d/b/a CONEMAUGH PHYSICIAN GROUP - OB/GYN ("Conemaugh Physician Group - Ob/Gyn") (collectively, "Defendants"), and allege, upon personal knowledge as to her own actions, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action to address Defendants' outrageous, illegal, and widespread practice of disclosing the confidential Personally Identifying Information[1] and/or

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

Protected Health Information[2] (collectively referred to as "Private Information") of Plaintiff and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook")[3] ("the Disclosure").

2. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace or denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

3. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the United States Department of Health and Human Services ("HHS") has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no

---

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). Defendants are each clearly a "covered entity" and some of the data compromised in this Disclosure that this action arises out of is "protected health information," subject to HIPAA.

[3] Facebook changed its name from Facebook, Inc. to Meta Platforms, Inc. in October 2021. Plaintiff's reference to both "Facebook" and "Meta" throughout this complaint refer to the same company

health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

4. Defendants are a Pennsylvania healthcare system, holding itself out as "...the largest healthcare provider in west central Pennsylvania, serving over a half-million patients each year through the Conemaugh Physician Group and Medical Staff, a network of hospitals, specialty clinics and patient focused programs. Conemaugh Health System employs over 5,000 clinical and non-clinical staff, and over 450 physicians committed to providing the ideal patient experience."[4]

5. In spite of its unique position as a massive and trusted healthcare provider, Defendants knowingly configured and implemented a software device known as a Tracking Pixel ("Pixel") to collect and transmit information from https://www.conemaugh.org/ (the "Website") to third parties, including information communicated in sensitive and presumptively confidential, billing portal, and related mobile applications (collectively "Online Platforms").

6. Defendants encourages its patients to use its Online Platforms for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, and more.

7. Plaintiff and other Class Members who used Defendants' Website thought they were communicating only with their trusted healthcare provider. Unbeknownst to Plaintiff and Class Members, however, Defendants has embedded the Facebook Tracking Pixel (the "Pixel" or "Facebook Pixel" or "Meta Pixel") on its Website, surreptitiously forcing Plaintiff and Class Members to transmit to Facebook every click, keystroke, and intimate detail about their medical treatment. Operating as designed and as implemented by Defendants, the Pixel allows the Private Information that Plaintiff and Class Members submit to Defendants to be unlawfully disclosed to

[4] https://www.conemaugh.org/about

Facebook alongside the individual's unique and persistent Facebook ID ("FID").[5]

8. A pixel is a piece of code that "tracks the people and [the] type of actions they take"[6] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), among other things.

9. The user's web browser executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Facebook Pixel is thus customizable and programmable, meaning that the website owner controls which of its webpages contain the Pixel and which events are tracked and transmitted to Facebook.

10. By installing the Facebook Pixel on its Website, Defendants effectively planted a bug on Plaintiff's and Class Members' web browsers and compelled them to disclose their communications with Defendants to Facebook.

11. In addition to the Facebook Pixel, Defendants also installed and implemented Facebook's Conversions Application Programming Interface ("CAPI") on its Website servers.[7]

12. Unlike the Facebook Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's

---

[5] The Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited: January 27, 2023)

[6] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Feb. 17, 2023).

[7] "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited: January 25, 2023).

browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.[8,9]

13. Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[10]

14. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendants to circumvent any ad blockers or other denials of consent by the website user that would prevent the Pixel from sending website users' Private Information to Facebook directly.

15. Defendants utilized the Pixel and CAPI data for marketing purposes in an effort to bolster its profits. The Facebook Pixel and CAPI are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiff's and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendants.

16. The information that Defendants' Tracking Pixel and CAPI sent to Facebook included the Private Information that Plaintiff and Class Members submitted to Defendants' Website, including for example, the type of medical treatment sought, the individual's particular

---

8 https://revealbot.com/blog/facebook-conversions-api/ (last visited: January 24, 2023).

9 "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel.... This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels.", https://developers.facebook.com/docs/marketing-api/conversions-api (last visited: January 27, 2023).

10 https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited: January 28, 2023).

health condition, and the fact that the individual attempted to or did book a medical appointment.

17. Such information allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers who geotarget Plaintiff's and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and CAPI. Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

18. Healthcare patients simply do not anticipate that their trusted healthcare provider will send personal health information or confidential medical information collected via its webpages to a hidden third party—let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the patients' consent.

19. Neither Plaintiff nor any other Class Member signed a written authorization permitting Defendants to send their Private Information to Facebook.

20. Despite willfully and intentionally incorporating the Facebook Pixel and CAPI into its Website and servers, Conemaugh Heath System has never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook. Plaintiff and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook as they communicated their confidential PHI with their healthcare provider via the Website, or stored on Defendants' servers to be later transmitted to Facebook so it could be used for targeted advertising and marketing purposes.

21. Defendants further made expressed and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of

communications that patients exchanged with Defendants.

22. Defendants owed common law, statutory, and regulatory duties to keep Plaintiff's and Class Members' communications and medical information safe, secure, and confidential.

23. Upon information and belief, Conemaugh Health System utilized the Pixel data to improve and to save costs on its marketing campaigns, improve its data analytics, and attract new patients.

24. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties to those individuals to protect and to safeguard that information from unauthorized disclosure.

25. Defendants breached their statutory and common law obligations to Plaintiff and Class Members by, *inter alia*,: (i) failing to adequately review its marketing programs and web based technology to ensure the hospital Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) aiding, agreeing, and conspiring with third-parties to intercept communications sent and received by Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook or others; (v) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Facebook Pixels; (vi) failing to warn Plaintiff and Class Members; and (vii) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

26. Plaintiff seek to remedy these harms and bring causes of action for (I) Invasion of Privacy, (II) Breach of Implied Contract, (III) Unjust Enrichment; (IV) Breach of Fiduciary Duty, (V) Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. § 20101 *et. seq.*, and (VI) Violation of the Pennsylvania Wiretapping and Electronic

Surveillance Control Act 18 Pa. C.S. § 5701 et seq., ("WESCA").

PARTIES

27. Plaintiff, Jane Doe is a natural person, resident, and a citizen of the Commonwealth of Pennsylvania, where she intends to remain, with a principal residence in Johnstown, Cambria County. She is a patient and former patient of Conemaugh Health System and a victim of Defendants' unauthorized disclosure of Private Information via the Meta Pixel.

28. Defendant, DLP Conemaugh Memorial Medical Center, LLC, is a Delaware limited liability company with its principal place of business in the Commonwealth of Pennsylvania at 1086 Franklin Steet, Johnstown, Pennsylvania 15905 in Cambria County, doing business as Conemaugh Health System d/b/a Conemaugh Memorial Medical Center (hereinafter "Conemaugh Health System").

29. Defendant, DLP Conemaugh Physician Practices, LLC d/b/a Conemaugh Physician Group - Ob/Gyn ("Conemaugh Physician Group - Ob/Gyn,") is a Delaware limited liability company with its principal place of business at 1111 Franklin Street, Suite 300, Johnstown, Pennsylvania 15905 in Cambria County (collectively with Conemaugh Health System "Defendants").

JURISDICTION AND VENUE

30. This Court has jurisdiction over the subject matter of this action pursuant to 42 Pa. Cons. Stat. § 931.

31. This Court has personal jurisdiction over Defendants pursuant to 42 Pa. Cons. Stat. § 5301, because Defendants each carry on of a continuous and systematic part of their general business within this Commonwealth and maintain principal places of business herein, and further upon information and belief as each have qualified as a foreign entity under the laws of

Pennsylvania.

32. Venue is appropriate in this Court under 231 Pa. Code § 2179, because Defendants' principal places of business are in Cambria County.

COMMON FACTUAL ALLEGATIONS

A. Background

33. Since 2014, Conemaugh Health System has owned and operated Conemaugh Memorial Medical Center whose headquarters and main campus are located at 1086 Franklin Street, Johnstown, Pennsylvania, 15905.

34. As described by Conemaugh Health System, Conemaugh Memorial Medical Center "is the flagship hospital of Conemaugh Health System," with over 500 beds, "[a] regional referral hospital known for clinical excellence, [and] home to the highest level of care designations for Neonatal Care (Level 3) and Trauma Care (Level 1)."[11]

35. At Conemaugh Memorial Medical Center, Conemaugh Health System, provides myriad medical, surgical, and other treatment services including care relating to Bariatrics & Weight Loss, Black Lung Screening, Brain & Spine, Cancer Care, Critical Care, Diabetes Care, Emergency & Trauma, Food and Nutrition Services, General Surgery, GI & Digestive Health, Heart & Vascular, Home Health & Hospice, diagnostic imaging, infusion, radiological services, laboratory services, maternity care, orthopedics, ostomy care, palliative care, plastic surgery, pulmonary care, rehabilitation services, treatment for sleep disorders, "spiritual care," stroke care, other surgical services, a Transitional Care Unit, Trauma Services, Women's Health care, and wound care.[12]

36. Moreover, within Conemaugh Memorial Medical Center, Conemaugh Physician

[11] https://www.conemaugh.org/conemaugh-memorial-medical-center
[12] *See Id.*

Group - Ob/Gyn provides obstetrics and gynecological medical treatment to patients at 1111 Franklin Street, Suite 300, Johnstown, PA 15905.

37. Collectively, Defendants serve their patients via its Online Platforms, which it encourages patients to use for finding providers, scheduling appointments and/or procedures, communicating with their healthcare providers, reviewing their medical histories and related documents, and communicating other information related to their treatment and status as a patient.

38. Notably, Defendants encourage patients and prospective patients find physicians through the "Find a Doctor" function of the Online Platforms, https://www.conemaugh.org/find-a-doctor, even as it cautions that many such healthcare providers are independent contractors and not hospital employees, representatives, or agents. This includes gynecologists who are employees and agents of Conemaugh Physician Group - Ob/Gyn.

39. Defendants promote the convenience and comprehensive functionality of its Online Platforms, allowing patients to find services and providers, schedule appointments, find medical information; as well as to utilize MyChart, stating that:

> Conemaugh Health System's online Patient Portal, **Conemaugh MyChart**, is available for all Conemaugh Health System and Conemaugh Physician Group patients. This **FREE** online tool provides access to personal health records -- anywhere, anytime![13]

40. Defendants use Conemaugh Health System's Website to connect Plaintiff and Class Members to Defendants' digital healthcare platforms with the goal of increasing profitability.

41. In furtherance of that goal, and to increase the success of its advertising and marketing, Defendants purposely installed the Facebook pixel and Facebook's Conversions API tools on many of its webpages within its Website and on its servers and programmed those webpages and servers. In doing so, Defendants surreptitiously shared patients' private and

[13] https://www.conemaugh.org/patient-portal

protected communications with Facebook, including communications that contain Plaintiff's and Class Members' Private Information.

42. To better understand Defendants' unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows:

i. Facebook's Business Tools and the Meta Pixel

43. As Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[14]

44. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendants, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

45. Facebook's Business Tools, including the Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

46. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"), as well as metadata, button clicks, and other information.[15] Businesses that want to target

---

[14] Facebook, *Meta Reports Fourth Quarter and Full Year 2021 Results* , https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022).

[15] Facebook, *Specifications for Facebook Pixel Standard Events*, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited Jan. 31, 2023); *see* Facebook, *Facebook Pixel, Accurate Event Tracking, Advanced*, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Facebook, *Best Practices for Facebook Pixel Setup*, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; Facebook, *App Events API*, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 31, 2023).

customers and advertise their services, such as Defendants, can track other user actions and can create their own tracking parameters by building a "custom event."[16]

47. One such Business Tool is the Pixel that "tracks the people and type of actions they take."[17] When a user accesses a webpage that is hosting the Pixel, the communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook—traveling from the user's browser to Facebook's server.

48. Notably, this transmission only occurs on webpages that contain the Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate privacy (such as the homepage) and disable it on pages that do implicate patient privacy (such as the "find a doctor" page). Thus, Plaintiff's and Class Member's Private Information would not have been disclosed to Facebook via the Pixel but for Defendants' decisions to install the Pixel on its Website and specifically on the webpages that solicit and receive Private Information.

49. The Meta Pixel's primary purpose is for marketing and ad targeting.[18]

50. Meta's own website informs companies that "The Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[19]

51. According to Meta, the Meta Pixel can collect the following data:

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page

---

[16] Facebook, *About Standard and Custom Website Events*, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* Facebook, *App Events API*, *supra*.

[17] Facebook, *Retargeting*, https://www.facebook.com/business/goals/retargeting.

[18] *See Meta Pixel*, META FOR DEVELOPERS https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

[19] *About Meta Pixel*, Meta Business Help Center. https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last accessed Mar. 19, 2023).

location, document, referrer and ***person using the website.*** (emphasis added).
Pixel-specific Data – Includes Pixel ID and the Facebook Cookie.

Button Click Data – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.

Optional Values – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.

Form Field Names – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[20]

52. Meta boasts to its prospective users that the Meta Pixel can be used to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.
- **Drive more sales**. Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.
- **Measure the results of your ads.** Better understand the impact of your ads by measuring what happens when people see them.[21]

53. Meta/Facebook likewise benefits from the data received from the Pixel and uses the data to serve targeted ads and identify users to be included in such targeted ads.

ii. Defendants' method of transmitting Plaintiff's and Class Members' Private Information via the Tracking Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Pixel

54. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g.,

[20] *Meta Pixel*, META FOR DEVELOPERS https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[21] *About Meta Pixel*, Meta Business Help Center. https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last accessed Mar. 19, 2023).

Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

55. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

56. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies.[22]

57. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), they also send the host server data, which is embedded inside the URL and can include cookies.

58. When an individual visits Defendants' Website, their web browser sends an HTTP Request to Defendants' servers that essentially asks Defendants' Website to retrieve certain information (such as Defendants' "Make an Appointment" page). Defendants' servers sends the HTTP Response, which contains the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendants' Website.

59. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

60. Source code may also command a web browser to send data transmissions to third

[22] "Cookies are small files of information that a web server generates and sends to a web browser. ...Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user, and this is exactly what happened when patients used Defendants' Website and Online Platforms.

61. Defendants' implementation of the Pixel is source code that acted much like a traditional wiretap, intercepting and transmitting communications intended only for Defendants.

62. Separate from the Pixel, Facebook and other website owners can place third-party cookies in the web browsers of users logged into their websites or services. These cookies can uniquely identify the user so the cookie owner can track the user as she moves around the internet—whether on the cookie owner's website or not. Facebook uses this type of third-party cookie when Facebook account holders use the Facebook app or website. As a result, when a Facebook account holder uses Defendants' Website, a unique id is sent to Facebook along with the intercepted communication that allows Facebook to identify the patient associated with the Private Information it has intercepted.

63. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. To counteract this, third parties bent on gathering data and Private Information implement workarounds that are difficult to detect or evade. Facebook's workaround is its Conversions API tool, which is particularly effective because the data transmitted via this tool does not rely on the website visitor's web browsers. Rather, the information travels directly from Defendants' server to Facebook's server.

64. Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]." Thus, Defendants receives and stores its communications with patients on its server before Conversions API collects and sends those communications—and the Private Information contained therein—to Facebook.

65. Notably, client devices do not have access to host servers and thus cannot prevent (or even detect) this additional transmission of information to Facebook.

66. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the host server, Facebook instructs companies like Defendants to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendants "to share website events [with Facebook] that the pixel may lose."[23] Thus, since Defendants implemented the Pixel in in accordance with Facebook's documentation, it is also reasonable to infer that Defendants implemented the Conversions API tool on its website.

67. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content on the host website. In other words, Facebook and others like it are not providing anything to the user relating to the user's communications. Instead, these third parties are typically procured to track user data and communications only to serve the marketing purposes of the website owner (*i.e.*, to bolster profits).

68. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendants can use its source code to commandeer its patients' computing devices, causing the device's web browser to contemporaneously and invisibly re-direct the patients' communications to hidden third parties like Facebook.

69. In this case, Defendants employed the Tracking Pixel and Conversions API to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook contemporaneously, invisibly, and without the patient's knowledge.

70. Consequently, when Plaintiff and Class Members visited Defendants' website and

[23] *See* https://www.facebook.com/business/help/308855623839366?id= 818859032317965 (last visited Jan. 23, 2023).

communicated their Private Information, including, but not limited to, medical treatment sought, medical conditions, appointment type and date, physician selected, specific button/menu selections, content (such as searches for symptoms or treatment options) typed into free text boxes, demographic information, email addresses, phone numbers, and emergency contact information, it is simultaneously intercepted and transmitted to Facebook.

iii. Defendants Violated Their own Privacy Policies

71. Conemaugh Health System maintains Patient Privacy Practices which apply to "***all*** Conemaugh Health System facilities and affiliates" (emphasis added).[24]

72. Defendants' Patient Privacy Practices provide, "[t]his notice describes how medical information about you may be used and disclosed and how you can get access to this information."[25]

73. The Patient Privacy Practices state, "**In these cases we never share your information unless you give us written permission:** • Marketing purposes. • Sale of your information…"[26]

74. Therein, Defendants further acknowledge, represents and promises:

> **Our Responsibilities**
>
> • We are required by law to maintain the privacy and security of your protected health information.
>
> • We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
>
> • We must follow the duties and privacy practices described in this notice and give you a copy of it.
>
> • We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any

[24] *See* Conemaugh Health System Patient Privacy Practices, available at https://www.conemaugh.org/sites/conemaugh/assets/uploads/Patient%20Privacy%20Practices%20rev.%202023.pdf (last accessed April 14, 2023) (attached hereto as **Exhibit A**).

[25] *Id*

[26] *Id.*

time. Let us know in writing if you change your mind. For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.[27]

75. Defendants' Notice of Privacy Practices does not permit Defendants to use and disclose Plaintiff's and Class Members' Private Information for marketing purposes without written permission.[28]

76. Defendants violated their own Patient Privacy Practices by unlawfully disclosing Plaintiff's and Class Members' Private Information to Facebook, Meta, Google, and likely other third parties.

77. Further, Defendants maintain an online privacy policy ("Online Privacy Policy")[29] provides:

> This Public Online Privacy Policy and the links included explain how we collect, treat, and protect your individually identifiable personal information. Specifically, the Public Online Privacy Statement describes how we handle the personal information that you submit to us when you submit a Contact Us form, attach a resume, and browse our website.
>
> [...]
>
> We've designed our public websites to capture two types of information: automatic tracking and individually identifiable personal information ("personal information").

78. The Online Privacy Policy goes onto explain that:

> Personal information can be anything you've provided through our public websites that identifies you. For example: Your name, email address, and street address are types of personal information. We store this information behind a complex series of firewalls, in a way that maximizes security and confidentiality.

79. Defendants' Online Privacy Policies promises that:

- We will only use the information to provide you with the services you have

---

[27] *Id.*
[28] *Id.*
[29] Conemaugh Health System website "Privacy Policy," available at https://www.conemaugh.org/privacy-policy **attached as Exhibit B.**

requested and as otherwise described in this Public Online Privacy Policy

- We will NOT sell, rent, or license the personal information you provide within our public websites.
- We do NOT provide any personally identifiable information about our users to any third party.
- Access to the data you submit is limited to the authorized staff detailed in our Site Disclaimer under Security.[30]

80. Defendants' Online Privacy Policy goes on to say:

> We use "cookies" to personalize our site for you and to collect aggregate information about site usage by all of our users. A cookie is a text file that our website transfers to your computer's hard drive for record keeping purposes. The cookie assigns a random, unique number to your computer. **It does not contain information that would personally identify you.**[31]

81. Defendants unlawfully disclosed Plaintiff's and Class Members' Private Information to Facebook, Meta, and likely other third parties, without authorization, in violation its own Patient Privacy Practices and Online Privacy Policy.

82. Defendants further misrepresented that they would preserve the confidentiality of their Private Information and the anonymity of their identities.

83. Despite the representations in its privacy policies, Defendants do indeed transfer PII and PHI, Private Information, to third parties. An example illustrates the point. If a user visits Defendants' website and clicks on the "Find a Doctor" tab (https://www.conemaugh.org/find-a-doctor), the individual's browser sends a request to Defendants' server requesting that it load the webpage. Because Defendants utilize the Facebook Pixel, Facebook's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, causing it to secretly duplicate the communication with Defendants, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

---

[30] *Id.* (emphasis in original).
[31] *Id* (emphases added)

84. For example, if the user clicks "Find a Doctor" and enters their Zip Code and the doctor's specialty, like "Addiction Medicine," this is information is shared with Facebook, Google, or others that Defendants has configured its Pixel to interact with.

85. After collecting and intercepting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

86. Every time Defendants send a patient's website activity data to Facebook, that patient's PII is also disclosed, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to the corresponding Facebook profile and the persons real world identity. A user who accesses Defendants' digital platforms while logged into Facebook will transmit the user cookie to Facebook, which contains that user's unencrypted Facebook ID.

87. Google and other companies likewise process this data in a similar manner and use it to connect the information to particular individuals to build marketing and other data profiles.

88. Through the Pixel, Defendants share their patients' identities and online activity, including personal information and search results related to their private medical treatment.

89. Defendants could have configured its tracking software to limit the information that it communicated to third parties, but it did not and instead intentionally selected the features and functionality of the Pixel that resulted in the Disclosure.

90. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendants to disclose their Private Information and assist with intercepting their communications. Plaintiff were

never provided with any written notice that Defendants discloses its patients' protected health information, nor were they provided any means of opting out of such disclosures. Defendants nonetheless knowingly disclosed Plaintiff's protected health information to Meta, Facebook, Google, and other unauthorized entities.

91. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

92. By law, Plaintiff are entitled to privacy in his protected health information and confidential communications. Defendants deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential communications, personally identifiable information, and protected health information; (2) disclosed patients' protected information to Facebook and others—unauthorized third-party eavesdroppers; and (3) undertook this pattern of conduct without notifying Plaintiff and Class Members and without obtaining their express written consent. Plaintiff did not discover that Defendants disclosed their personally identifiable information and protected health information to Facebook and Google, and assisted Facebook and Google with intercepting their communications.

B. Plaintiff's Experience

93. Plaintiff Jane Doe is a patient of Defendants, receiving services both at Conemaugh Health System's Conemaugh Memorial Medical Center, and within their physician's

network at Conemaugh Physician Group - Ob/Gyn that relied on Defendant's digital healthcare platforms to communicate confidential patient information.

94. Plaintiff accessed Defendants' digital tools to receive healthcare services from Defendants and at Defendants' direction and encouragement, to find physicians, to find different hospital locations, to check her test results, to communicate with physicians, and confirm appointments. Plaintiff last used these digital tools on April 13, 2023, to check her test results.

95. Plaintiff reasonably expected that her online communications with Defendants were confidential, solely between herself and Defendants, and that such communications would not be transmitted to or intercepted by a third party.

96. Plaintiff provided his Private Information to Defendants and trusted that the information would be safeguarded according to Conemaugh Health System's privacy policies and state and federal law.

97. As described herein, Defendants sent Plaintiff's Private Information to Facebook, Google, and others when she used Defendants' digital platforms to communicate healthcare and identifying information to Defendants.

98. Pursuant to the process described herein, Defendants assisted Facebook, Google, and others with intercepting Plaintiff Jane Doe's communications, including those that contained PII, PHI, and related confidential information. Defendants facilitated these interceptions without Plaintiff Jane Doe's knowledge, consent, or express written authorization.

99. By failing to receive the requisite consent, Defendants breached confidentiality and unlawfully disclosed Plaintiff Jane Doe's Private Information, PII and PHI.

C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI

100. In June 2020, after promising users that app developers would not have access to

data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[32] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

101. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective … at preventing the receipt of sensitive data."[33]

102. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data is not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[34] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and

[32] https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/
[33] https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf
[34] https://slate.com/technology/2022/06/health-data-brokers-privacy.html

Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[35]

103. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[36]

104. Furthermore, in June 2022, an investigation by The Markup[37] revealed that the Meta Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[38] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[39] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[40]

105. The Markup article found during the course of its investigation that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital

---

[35] https://slate.com/technology/2022/06/health-data-brokers-privacy.html
[36] https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes
[37] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* www.themarkup.org/about (last accessed Mar. 19, 2023).
[38] PIXEL HUNT, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last accessed Mar. 19, 2023).
[39] *Id.*
[40] *Id.*

websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[41]

106. Despite knowing that the Meta Pixel code embedded in its websites was sending patients' personal health information, Private Information, to Facebook, Defendants did nothing to protect its patients from egregious intrusions into its patients' privacy, choosing instead to benefit at those patients' expense.

107. In addition to the 33 hospitals identified by The Markup that had installed the Meta Pixel on their websites, The Markup identified seven health systems that had installed the pixels inside their password-protected patient portals.[42]

108. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply troubled" by what the hospitals were doing by capturing patient data and sharing it.[43]

D. Defendants Violated HIPAA Standards

109. Under Pennsylvania law and HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[44]

110. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

111. In Guidance regarding Methods for De-identification of Protected Health

---

[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[45]

112. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).[46]

113. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[47]

114. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[48]

---

[45] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 3, 2022).
[46] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Nov. 3, 2022)
[47] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.
[48] *Id.*

115. Citing The Markup's June 2022 article, the Bulletin expressly notes:

> Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
>
> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule.[49]

116. In other words, HHS has expressly stated that Defendants' conduct of implementing the Facebook Pixel is a violation of HIPAA Rules.

E. Defendants Violated Industry Standards

117. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

118. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications, which are applicable to Defendants, and their physicians.

119. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including,

[49] *Id.* (emphasis in original) (internal citations omitted).

... personal data (informational privacy).

120. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

121. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically...must...:(c) release patient information only in keeping ethics guidelines for confidentiality.

F. Plaintiff's and Class Members' Expectation of Privacy

122. Plaintiff and Class Members were aware of Defendants' duty of confidentiality when they sought medical services from Defendants.

123. Indeed, at all times when Plaintiff and Class Members provided their Private Information to Defendants, they all had a reasonable expectation that the information would remain private and that Defendants would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

G. IP Addresses are Personally Identifiable Information

124. On information and belief, through the use of the Facebook Pixel on Defendants' Website, Defendants also disclosed and otherwise assisted Facebook with intercepting Plaintiff's and Class Members' Computer IP addresses.

125. An IP address is a number that identifies the address of a device connected to the Internet.

126. IP addresses are used to identify and route communications on the Internet.

127. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

128. Facebook tracks every IP address ever associated with a Facebook user.

129. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

130. Under HIPAA, an IP address is considered personally identifiable information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. See 45 C.F.R. § 164.514 (2).

- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

131. Consequently, by disclosing IP addresses, Defendants' business practices violated HIPAA and industry privacy standards.

H. Defendants Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures

132. The sole purpose of the use of the Facebook Pixel on Defendants' Website was marketing and profits.

133. In exchange for disclosing the Private Information of its patients, Defendants is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on its platform.

134. Retargeting is a form of online marketing that targets users with ads based on their

previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendants re-targeted patients and potential patients.

135. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendants.

I. Plaintiff's and Class Members' Private Information Had Financial Value

136. Plaintiff's data and Private Information has economic value. Facebook regularly uses data that it acquires to create Core and Custom Audiences, as well as Lookalike Audiences and then sells that information to advertising clients.

137. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

138. The value of health data in particular is well-known, and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[50]

139. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[51]

---

[50] *See* https://time.com/4588104/medical-data-industry/ (last visited February 16, 2023).
[51] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited February 16, 2023).

CLASS ALLEGATIONS

140. Plaintiff brings this nationwide class action on behalf of themselves and on behalf of other similarly situated persons.

141. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All persons whose Private Information was disclosed by Defendants to third parties through the Meta Pixel and related technology without authorization.

142. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

143. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

144. **Numerosity:** Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly accessed in the Disclosure, and each Class is apparently identifiable within Defendants' records.

145. **Commonality:** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect Plaintiff's and Class Members' Private Information;

b. Whether Defendants had duties not to disclose the Plaintiff's and Class Members'

Private Information to unauthorized third parties;

c. Whether Defendants had duties not to use Plaintiff's and Class Members' Private Information for non-healthcare purposes;

d. Whether Defendants had duties not to use Plaintiff's and Class Members' Private Information for unauthorized purposes;

e. Whether Defendants failed to adequately safeguard Plaintiff's and Class Members' Private Information;

f. Whether and when Defendants actually learned of the Disclosure;

g. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

h. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

i. Whether Defendants failed to properly implement and configure the tracking software on its digital platforms to prevent the disclosure of information compromised in the Disclosure;

j. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Disclosure to occur;

k. Whether Defendants engaged in unfair, unlawful, or deceptive practices by misrepresenting that it would safeguard Plaintiff's and Class Members' Private Information;

146. **Typicality:** Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Disclosure, due to Defendants' use and incorporation of the tracking software.

147. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendants has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

148. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff have suffered are typical of other Class Members. Plaintiff have also retained counsel experienced in complex class action litigation, and Plaintiff intend to prosecute this action vigorously.

149. **Superiority and Manageability:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

150. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

151. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

152. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

153. Unless a Class-wide injunction is issued, Defendants may continue in its unlawful disclosure and failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Disclosure, and Defendants may continue to act unlawfully as set forth in this Complaint.

154. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

155. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. Whether an implied contract existed between Defendants on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Disclosure;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
INVASION OF PRIVACY--INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

156. Plaintiff realleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

157. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendants, Conemaugh Health System and Conemaugh Physician Group - Ob/Gyn

158. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendants via their website and the communications platforms and services therein.

159. Plaintiff and Class Members communicated sensitive PHI and PII that they intended for only Defendants to receive and that they understood Defendants would keep private.

160. Defendants' disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and Class Members is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion and their private affairs and concerns.

161. Plaintiff and Class Members had a reasonable expectation of privacy given Defendants' representations, Notice of Privacy Practices, Terms of Use, and HIPAA. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding

healthcare with their healthcare providers will be kept confidential. Defendants' disclosure of PHI coupled with PII is highly offensive to the reasonable person.

162. As a result of Defendants' actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

163. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages.

164. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

165. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendants' actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendants from engaging in such conduct in the future.

166. Plaintiff also seek such other relief as the Court may deem just and proper.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

167. Plaintiff realleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

168. Defendants required Plaintiff and the Class Members to provide their Private Information, including full names, email addresses, phone numbers, computer IP addresses, appointment information, medical insurance information, medical provider information, medical histories, and other content submitted on Defendants' website and billing portal as a condition of

their receiving healthcare services.

169. As a condition of utilizing Defendants' digital platforms and receiving services from Defendants, Plaintiff and the Class provided their Private Information and compensation for their medical care. In so doing, Plaintiff and the Class entered into contracts with Defendants by which Defendants agreed to safeguard and protect such information, in its Privacy Practices and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

170. Implicit in the agreement between Defendants and their patients was the obligation that both parties would maintain the Private Information confidentially and securely.

171. Defendants had an implied duty of good faith to ensure that the Private Information of Plaintiff and Class Members in its possession was only used only as authorized, such as to provide medical treatment, billing, and other medical benefits from Conemaugh Health System and Conemaugh Physician Group - Ob/Gyn.

172. Defendants had an implied duty to protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses.

173. Additionally, Conemaugh Health System and Conemaugh Physician Group - Ob/Gyn implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

174. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendants, Conemaugh Health System and Conemaugh Physician Group - Ob/Gyn. Defendants did not. Plaintiff and Class Members would not have provided their confidential Private Information to Defendants in the absence of their implied contracts with Defendants and would have instead retained the opportunity to control their Private Information for uses other than

medical treatment, billing, and benefits from Conemaugh Health System and Conemaugh Physician Group - Ob/Gyn.

175. Defendants breached the implied contracts with Plaintiff and Class members by disclosing Plaintiff's and Class Members' Private Information to an unauthorized third party.

176. Defendants' acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiff and Class Members to provide their Private Information in exchange for medical treatment and benefits.

177. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiff and the Class have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities.

178. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

179. Plaintiff realleges and incorporate the preceding paragraphs of this Complaint as if fully set forth herein.

180. This claim is pleaded solely in the alternative to Count II.

181. Plaintiff and Class members conferred a monetary benefit upon Defendants, Conemaugh Health System and Conemaugh Physician Group - Ob/Gyn in the form of valuable sensitive medical information that Defendants collected from Plaintiff and Class Members under the guise of keeping this information private. Defendants collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiff and the Class Members conferred a benefit on

Defendants in the form of monetary compensation.

182. Plaintiff and Class Members would not have used Defendants' services or would have paid less for those services, if they had known that Defendants would collect, use, and disclose this information to third parties.

183. Defendants appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class members.

184. As a result of Conemaugh Health System's and Conemaugh Physician Group - Ob/Gyn's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

185. The benefits that Defendants derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles for Defendants to be permitted to retain any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

186. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of its conduct and the Disclosure alleged herein.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

187. Plaintiff realleges and incorporate the preceding paragraphs of this Complaint as

if fully set forth herein.

188. A relationship existed between Plaintiff and the Class on the one hand and Defendants on the other in which Plaintiff and the Class put their trust in Defendants, Conemaugh Health System and Conemaugh Physician Group - Ob/Gyn, to protect the Private Information of Plaintiff and the Class and Defendants accepted that trust.

189. Defendants breached the fiduciary duty that it owed to Plaintiff and the Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect, and intentionally disclosing, the Private Information of Plaintiff and the Class.

190. Defendants' breach of fiduciary duty was a legal cause of damage to Plaintiff and the Class.

191. But-for Defendants' breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred.

192. Defendants' breach of fiduciary duty contributed substantially to producing the damage to the Plaintiff and the Class.

193. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiff and Class Members are entitled to and do demand actual, consequential, and nominal damages, injunctive relief, and all other relief allowed by law.

COUNT V
VIOLATION OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 PA. STAT. § 20101 *ET. SEQ.* ("UTPCPL")
(On Behalf of Plaintiff and the Class)

194. Plaintiff realleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

195. Plaintiff, the members of the Class, and Defendant are all "persons" within the meaning of the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), 73 Pa. Stat. § 201-2(2).

196. The UTPCPL prohibits "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."

197. Under the UTPCPL, "[u]nfair or deceptive acts or practices" include: "[r]epresenting that… services have sponsorship, approval, characteristics, . . . [or] benefits . . . that they do not have," 73 Pa. § 201-2(4)(v); "[r]epresenting that… services are of a particular standard . . . [or] quality . . . if they are of another," *id.* § 201-2(4)(vii); "[a]dvertising… services with intent not to sell them as advertised," *id.* § 201-2(4)(ix); and "[e]ngaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding," *id.* § 201-2(4)(xxi).

198. Defendants' acts, practices, and omissions alleged in this Complaint constitute unlawful, unfair, and deceptive acts and practices under the UTPCPL.

199. Defendants knew or should have known about the unauthorized disclosure of Plaintiff's and the Class's Private Information via the Meta Pixel, yet Defendants concealed that information from Plaintiff and the Class.

200. Defendants engaged in unlawful, unfair, and deceptive acts and practices prohibited by the UTPCPL by, among other things: misrepresenting or omitting material facts to Plaintiff and the Class regarding the adequacy of Defendants' protection of their Private Information, in violation of 73 Pa. Stat. §§ 201-(4)(v), (vii), (ix), and (xxi);

201. Defendants' acts and omissions and its misrepresentations were intentional, knowing, and undertaken to mislead the public, including Plaintiff and the members of the Class.

202. Defendants' unlawful, unfair, and deceptive acts and practices were unethical, oppressive, and unscrupulous. These acts and practices caused substantial injury to Plaintiff and members of the Class that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

203. Defendants possessed exclusive knowledge about the disclosure of Plaintiff's and the Class Member's Private Information to unauthorized parties via the Meta Pixel to their detriment.

204. Defendants had a duty to disclose the foregoing to Plaintiff and members of the Class, and failed to do so.

205. Plaintiff and members of the Class reasonably relied on Defendants to protect and safeguard their Private Information and to promptly and adequately inform them of the unauthorized Disclosure.

206. Defendants owed Plaintiff and the Class a duty to: maintain the privacy and security of Plaintiff's and the Class's Private Information; take proper action to prevent the Disclosure; take proper action following the Disclosure to protect further unauthorized disclosure, release, and theft of Private Information, and promptly inform Plaintiff and members of the Class about the breach.

207. Plaintiff and members of the Class suffered ascertainable losses of money or property as a result of Defendants' use and employment of methods, acts, or practices declared to be unlawful by 73 Pa. §§ 201-2(2) and 201-(3).

208. Plaintiff and the Class seek an order enjoining Defendants' unlawful acts and practices and awarding any other just and proper relief available under the UTPCPL including actual or statutory damages, treble damages, and attorneys' fees and costs.

COUNT VI
VIOLATION OF THE PENNSYLVANIA WIRETAPPING AND ELECTRONIC SURVEILLANCE CONTROL ACT 18 PA. C.S. § 5701, *ET SEQ.* ("WESCA")
(On Behalf of Plaintiff and the Class)

209. Plaintiff realleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

210. WESCA defines "Person" as any employee, or agent of the United States or any state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust or corporation. 18 Pa. C.S.A. § 5702.

211. Defendants each constitute a "person" under WESCA, 18 Pa. C.S.A. § 5702.

212. The Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S.A. §§ 5701, 5703(1) ("WESCA") prohibits any person from willfully intercepting, endeavoring to intercept, or procuring of any other person to intercept or endeavor to intercept, any wire, electronic, or oral communication.

213. WESCA, 18 Pa. C.S.A. § 5702 defines "intercept," as "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. C.S.A. § 5702.

214. WESCA, 18 Pa. C.S.A. § 5703(2)-(3) also prohibits the disclosure of, or use of, the contents of any wire, electronic, or oral communication, or any evidence derived therefrom, with knowledge that the information was obtained through the interception of a wire, electronic, or oral communication.

215. WESCA, 18 Pa. C.S.A. § 5741(a) further prohibits the knowing access without

authorization of a facility through which an electronic communication is provided or exceeds an authorization to access that facility and obtains, or alters access to a wire or electronic communication while that communication is in electronic storage.

216. WESCA, 18 Pa. C.S.A. § 5741, is also violated where, for the purpose of commercial advantage or private commercial gain, a person knowingly accesses without authorization a facility through which an electronic communication service is provided, or exceed access to that facility, and obtains access to a wire or electronic communication while that communication is in electronic storage.

217. As set forth herein, Defendants knowingly, willfully, and intentionally intercepted and disclosed Plaintiffs' and Class Members' electronic communications, without the consent of the Plaintiffs and Class Members, using Facebook's tracking devices.

218. Defendants knowingly, willfully, and intentionally intercepted Plaintiffs' and Class Members' electronic communications for the purpose of disclosing those communications to third parties including Facebook without the knowledge, consent, or written authorization of Plaintiffs or Class Members.

219. The devices used in this case, include, but are not limited to:

a. to which Plaintiffs' and Class Members' communications were disclosed.

b. Plaintiffs' and Class Members' personal computing devices;

c. Plaintiffs' and Class Members' web browsers;

d. Plaintiffs' and Class Members' browser-managed files;

e. Facebook's Pixel;

f. Internet cookies;

g. Defendant's computer servers;

h. Third-party source code utilized by Defendant; and

i. Computer servers of third parties (including Facebook)

220. Defendants aided in the interception of communications between Plaintiffs and Class Members and Defendant that were redirected to and recorded by third parties without the Plaintiffs or Class Members consent.

221. WESCA confers a private civil cause of action to any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation thereof against "any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. C.S. § 5725(a).

222. As a result of Defendants violations of WESCA, pursuant to 18 Pa. C.S.A. § 5725(a), Plaintiff and the Class Members are entitled to recover actual damages that are not less than liquidated damages computed at a rate of $100.00 a day for each day of violation or $1,000.00, whichever is higher; punitive damages; and reasonable attorneys' fees and other litigation costs reasonably incurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, JANE DOE, Individually, and on behalf of all others similarly situated, pray for judgment as follows:

A. For an Order certifying this action as a Class action and appointing Plaintiff as Class Representatives and Plaintiff's counsel as Class Counsel;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Sensitive Information compromised during the Disclosure;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

E. Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law, including pursuant to the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. § 20101, *et seq.* ("UTPCPL"), and the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S.A. §§ 5701, *et seq.* ("WESCA");

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees under the UTPCPL, WESCA, the common fund doctrine, and any other applicable law;

I. Costs and any other expense, including expert witness fees incurred by Plaintiff in connection with this action;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Trial by jury on all issues so triable; and,

L. Such other and further relief as this court may deem just and proper.

Dated: April 17, 2023

Respectfully submitted,

SALTZ MONGELUZZI & BENDESKY P.C.

By: */s/ Elizabeth A. Bailey*

Elizabeth A. Bailey (Identification No. 316689)
SALTZ MONGELUZZI & BENDESKY P.C.
52nd Floor
1650 Market Street
Philadelphia, Pennsylvania 19103
(215) 496-8282
ebailey@smbb.com

Lynn A. Toops (*Pro Hac Vice* forthcoming)
Amina A. Thomas (*Pro Hac Vice* forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina C. Borelli (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class

EXHIBIT A

Conemaugh Health System

Your Information. Your Rights. Our Responsibilities

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. This notice applies to all Conemaugh Health System facilities and affiliates.

Your Rights

You have the right to:
- Get a copy of your paper or electronic medical record
- Correct your paper or electronic medical record
- Request confidential communication
- Ask us to limit the information we share
- Get a list of those with whom we've shared your information
- Get a copy of this privacy notice
- Choose someone to act for you
- File a complaint if you believe your privacy rights have been violated

Your Choices

You have some choices in the way that we use and share information as we:
- Tell family and friends about your condition
- Provide disaster relief
- Include you in a hospital directory
- Provide mental health care
- Market our services and sell your information
- Raise funds

Our Uses and Disclosures

We may use and share your information as we:
- Treat you
- Run our organization
- Bill for your services
- Help with public health and safety issues
- Do research
- Comply with the law
- Respond to organ and tissue donation requests
- Work with a medical examiner or funeral director
- Address workers' compensation, law enforcement, and other government requests
- Respond to lawsuits and legal actions

Your Rights

When it comes to your health information, you have certain rights. This section explains your rights and some of our responsibilities to help you.

Get an electronic or paper copy of your medical record
- You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this.
- We will provide a copy or a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost-based fee.

Ask us to correct your medical record
- You can ask us to correct health information about you that you think is incorrect or incomplete. Ask us how to do this.
- We may say "no" to your request, but we'll tell you why in writing within 60 days.

Request confidential communications
- You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.
- We will say "yes" to all reasonable requests.

Ask us to limit what we use or share
- You can ask us not to use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request, and we may say "no" if it would affect your care.
- If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. We will say "yes" unless a law requires us to share that information.

Get a list of those with whom we've shared information
- You can ask for a list (accounting) of the times we've shared your health information for six years prior to the date you ask, who we shared it with, and why.
- We will include all the disclosures except for those about treatment, payment, and health care operations, and certain other disclosures (such as any you asked us to make). We'll provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.

Get a copy of this privacy notice
You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.

Choose someone to act for you
- If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.
- We will make sure the person has this authority and can act for you before we take any action.

File a complaint if you feel your rights are violated
- You can complain if you feel we have violated your rights by contacting us using the information on page 1.
- You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting www.hhs.gov/ocr/privacy/hipaa/complaints/.
- We will not retaliate against you for filing a complaint.

Your Choices

For certain health information, you can tell us your choices about what we share. If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

In these cases, you have both the right and choice to tell us to:
- Share information with your family, close friends, or others involved in your care
- Share information in a disaster relief situation
- Include your information in a hospital directory

If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.

In these cases we never share your information unless you give us written permission:
- Marketing purposes
- Sale of your information
- Most sharing of psychotherapy notes

In the case of fundraising:
- We may contact you for fundraising efforts, but you can tell us not to contact you again.

Our Uses and Disclosures

How do we typically use or share your health information?
We typically use or share your health information in the following ways.

Treat you
We can use your health information and share it with other professionals who are treating you.
Example: A doctor treating you for an injury asks another doctor about your overall health condition.

Run our organization
We can use and share your health information to run our practice, improve your care, and contact you when necessary.
Example: We use health information about you to manage your treatment and services.

Bill for your services
We can use and share your health information to bill and get payment from health plans or other entities.
Example: We give information about you to your health insurance plan so it will pay for your services.

How else can we use or share your health information?
We are allowed or required to share your information in other ways – usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes.
For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.

Help with public health and safety issues
We can share health information about you for certain situations such as:
- Preventing disease
- Helping with product recalls
- Reporting adverse reactions to medications
- Reporting suspected abuse, neglect, or domestic violence
- Preventing or reducing a serious threat to anyone's health or safety

Do research
We can use or share your information for health research.

Comply with the law
We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we're complying with federal privacy law.

Respond to organ and tissue donation requests
We can share health information about you with organ procurement organizations.

Work with a medical examiner or funeral director
We can share health information with a coroner, medical examiner, or funeral director when an individual dies.

Address workers' compensation, law enforcement, and other government requests we can use or share health information about you:
- For workers' compensation claims
- For law enforcement purposes or with a law enforcement official
- With health oversight agencies for activities authorized by law
- For special government functions such as military, national security, and presidential protective services

Respond to lawsuits and legal actions
We can share health information about you in response to a court or administrative order, or in response to a subpoena.

Our Responsibilities

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.

Changes to the Terms of this Notice
We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request, in our office, and on our web site.

Conemaugh Health System's online Patient Portal, **Conemaugh MyChart**, is available for all Conemaugh Health System and Conemaugh Physician Group patients. This **FREE** online tool provides access to personal health records anywhere, anytime! Register at conemaugh.org/MyChart.

Conemaugh Health System Privacy Officer
814.410.8421

Making Communities Healthier

Conemaugh Health System
Duke LifePoint Healthcare

Original Notice date - April 2003 • Revised August 2010 • Revised May 2013. • Revised August 2013 • Revised April 2018 • January 2023

EXHIBIT B

Privacy Policy

Your privacy is important to us.

This Public Online Privacy Policy and the links included explain how we collect, treat, and protect your individually identifiable personal information. Specifically, the Public Online Privacy Statement describes how we handle the personal information that you submit to us when you submit a Contact Us form, attach a resume, and browse our website.

1. Information we collect:

We've designed our public websites to capture two types of information: automatic tracking and individually identifiable personal information ("personal information"). The first allows us to see which topics interest you most; the second helps us provide the services you requested.

- Automatic tracking information is gathered by following your "footsteps" online. Most web browsers automatically provide this information to the sites they visit and display. This information is not personally identifiable. We do not collect any additional data from your computer, and we do not compare data provided by your browser with any other data we maintain. The routes you—and other visitors—choose helps us learn about the people who visit our sites. We use aggregate numbers to compile statistics, monitor trends and track site usage. We also use the information to make sure our technology is compatible with yours. We're then better able to offer content, products and services that match your needs.
- Personal information can be anything you've provided through our public websites that identifies you. For example: Your name, email address, and

street address are types of personal information. We store this information behind a complex series of firewalls, in a way that maximizes security and confidentiality.

2. Information we collect:

- We will only use the information to provide you with the services you have requested and as otherwise described in this Public Online Privacy Policy
- We will NOT sell, rent, or license the personal information you provide within our public websites.
- We do NOT provide any personally identifiable information about our users to any third party.
- Access to the data you submit is limited to the authorized staff detailed in our Site Disclaimer under Security.

3. Use of cookies:

We use "cookies" to personalize our site for you and to collect aggregate information about site usage by all of our users. A cookie is a text file that our website transfers to your computer's hard drive for record keeping purposes. The cookie assigns a random, unique number to your computer. It does not contain information that would personally identify you.

SALTZ MONGELUZZI BENDESKY
TRIAL LAWYERS

DELAWARE COUNTY OFFICE
20 WEST THIRD STREET
P.O. BOX 1670
MEDIA, PA 19063
VOICE 610.627.9777
FAX 610.627.9787

ONE LIBERTY PLACE, 52ND FLOOR
1650 MARKET STREET
PHILADELPHIA, PA 19103
VOICE 215.496.8282
FAX 215.496.0999

NEW JERSEY OFFICE
8000 SAGEMORE DRIVE
SUITE 8303
MARLTON, NJ 08053
VOICE 856.751.8383
FAX 856.751.0868

MONTGOMERY COUNTY OFFICE
120 GIBRALTAR RD
SUITE 218
HORSHAM, PA 19044
VOICE 215.496.8282
FAX 215.754.4443

ELIZABETH A. BAILEY
DIRECT DIAL 215-575-3859
EBAILEY@SMBB.COM

April 17, 2023

Via Fed Ex – No. 816388140574

Cambria County Prothonotary's Office
200 South Center Street
Ebensburg, PA 15931

Re: ***COMPLAINT – DOE V. DLP CONEMAUGH MEMORIAL MEDICAL CENTER, LLC D/B/A CONEMAUGH HEALTH SYSTEM D/B/A CONEMAUGH MEMORIAL MEDICAL CENTER***

To Whom It May Concern:

Enclosed please find two copies of a Complaint. Please file the attached Complaint with Exhibits. Kindly time stamp the cover of the second copy and return in the self-addressed and stamped envelope. Enclosed please also find a check for $104.75 for filing fees.

Sincerely,
Elizabeth Bailey, Esq.

SALTZ MONGELUZZI & BENDESKY P.C.
BY: ELIZABETH A. BAILEY
ONE LIBERTY PLACE, 52ND FLOOR
1650 MARKET STREET
PHILADELPHIA, PA 19103
(215) 496-8282

COHEN & MALAD, LLP
BY: LYNN TOOPS/AMINA A. THOMAS
PRO HAC VICE PENDING
ONE INDIANA SQUARE, SUITE 1400
INDIANAPOLIS, IN 46204
(317) 636-6481

TURKE & STRAUSS LLP
BY: RAINA C. BORRELLI/SAMUEL J. STRAUSS
PRO HAC VICE PENDING
613 WILLIAMSON STREET, SUITE 201
MADISON, WI 53703
(608) 237-1775

STRANCH, JENNINGS & GARVEY, PLLC
J. GERARD STRANCH, IV/ANDREW E. MIZE
PRO HAC VICE PENDING
223 ROSA L. PARKS AVENUE, SUITE 200
NASHVILLE, TN 37203
(615) 254-8801

Attorneys for Plaintiff

CAMBRIA COUNTY COURT OF COMMON PLEAS

JANE DOE **Individually, and on behalf of all others similarly situated,** ***Plaintiff,*** **v.** **DLP CONEMAUGH MEMORIAL MEDICAL CENTER, LLC D/B/A CONEMAUGH HEALTH SYSTEM D/B/A CONEMAUGH MEMORIAL MEDICAL CENTER**	)	Case No. 2023-1430 JURY TRIAL DEMANDED

D/B/A CONEMAUGH MEMORIAL MEDICAL CENTER
1086 Franklin Street
Johnstown, Pennsylvania 15905

-and-

DLP CONEMAUGH PHYSICIAN PRACTICES, LLC D/B/A CONEMAUGH PHYSICIAN GROUP - OB/GYN
1111 Franklin Street
Suite 300
Johnstown, Pennsylvania 15905

Defendants.

NOTICE	AVISO
"You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by an attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you. "YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DO NOT HAVE A LAWYER OR CANNOT AFFORD ONE, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT WHERE YOU CAN GET LEGAL HELP. THIS OFFICE CAN PROVIDE YOU WITH INFORMATION ABOUT HIRING A LAWYER. IF YOU CANNOT AFFORD TO HIRE A LAWYER, THIS OFFICE MAY BE ABLE TO PROVIDE YOU WITH INFORMATION ABOUT AGENCIES THAT MAY OFFER LEGAL SERVICES TO ELIGIBLE PERSONS AT A REDUCED FEE OR NO FEE. CAMBRIA COUNTY BAR ASSOCIATION LAWYER REFERRAL SERVICE 200 South Center Street Ebensburg, PA 15931 (814) 255-3221	"Le han demandado en corte. Si usted quiere defenderse contra las demandas nombradas en las páginas siguientes, tiene veinte (20) dias, a partir de recibir esta demanda y la notificatión para entablar perSonsalmente o por un abogado una compareceencia escrita y tambien para entablar con la corte en forma escrita sus defensas y objeciones a las demandas contra usted. Sea avisado que si usted no se defiende, el caso puede continuar sin usted y la corte puede incorporar un juicio contra usted sin previo aviso para conseguir el dinero demandado en el pleito o para conseguir culquier otra demanda o alivio solicitados por el demandante. Usted puede perder dinero o propiedad u otros derechos importantes para usted. USTED DEBE LLEVAR ESTE DOCUMENTO A SU ABOGADO INMEDIATAMENTE. SI USTED NO TIENE ABOGADO (O NO TIENE DINERO SUFICIENTE PARA PARGAR A UN ABOGADO), VAYA EN PERSONSA O LLAME POR TELEFONO LA OFICINA NOMBRADA ABAJO PARA AVERIGUAR DONDE SE PUEDE CONSEGUIR ASSISTENCIA LEGAL. ESTA OFICINA PUEDE PROPORCIONARLE LA INFORMACION SOBRE CONTRATAR A UN ABOGADO. SI USTED NO TIENE DINERO SUFICIENTE PARA PAGAR A UN ABOGADO, ESTA OFICINA PUEDE PROPORCIONARLE INFORMACION SOBRE AGENCIAS QUE OFRECEN SERVICIOS LEGALES A PERSONSAS QUE CUMPLEN LOS REQUISITOS PARA UN HONORARIO REDUCIDO O NINGUN HONORARIO. CAMBRIA COUNTY BAR ASSOCIATION LAWYER REFERRAL SERVICE 200 South Center Street Ebensburg, PA 15931 (814) 255-3221

AMENDED CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff, JANE DOE, Individually, and on behalf of all others similarly situated (hereinafter "Plaintiff") brings this Amended Class Action Complaint against the Defendants, DLP CONEMAUGH MEMORIAL MEDICAL CENTER, LLC, d/b/a Conemaugh Health System d/b/a Conemaugh Memorial Medical Center ("Conemaugh Health System"), and DLP CONEMAUGH PHYSICIAN PRACTICES, LLC d/b/a CONEMAUGH PHYSICIAN

GROUP - OB/GYN ("Conemaugh Physician Group - Ob/Gyn") (collectively, "Defendants"), and allege, upon personal knowledge as to her own actions, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action to address Defendants' outrageous, illegal, and widespread practice of disclosing the confidential Personally Identifying Information[1] and/or Protected Health Information[2] (collectively referred to as "Private Information") of Plaintiff and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook")[3] ("the Disclosure").

2. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace or denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems down the

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). Defendants are each clearly a "covered entity" and some of the data compromised in this Disclosure that this action arises out of is "protected health information," subject to HIPAA.

[3] Facebook changed its name from Facebook, Inc. to Meta Platforms, Inc. in October 2021. Plaintiff's reference to both "Facebook" and "Meta" throughout this complaint refer to the same company

road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

3. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the United States Department of Health and Human Services ("HHS") has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

4. Defendants are a Pennsylvania healthcare system, holding itself out as "...the largest healthcare provider in west central Pennsylvania, serving over a half-million patients each year through the Conemaugh Physician Group and Medical Staff, a network of hospitals, specialty clinics and patient focused programs. Conemaugh Health System employs over 5,000 clinical and non-clinical staff, and over 450 physicians committed to providing the ideal patient experience."[4]

5. In spite of its unique position as a massive and trusted healthcare provider, Defendants knowingly configured and implemented a software device known as a Tracking Pixel ("Pixel") to collect and transmit information from https://www.conemaugh.org/ (the "Website") to third parties, including information communicated in sensitive and presumptively confidential billing portal, and related mobile applications (collectively "Online Platforms").

6. Defendants encourages its patients to use its Online Platforms for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms,

[4] https://www.conemaugh.org/about

searching medical conditions and treatment options, and more.

7. Plaintiff and other Class Members who used Defendants' Website thought they were communicating only with their trusted healthcare provider. Unbeknownst to Plaintiff and Class Members, however, Defendants has embedded the Facebook Tracking Pixel (the "Pixel" or "Facebook Pixel" or "Meta Pixel") on its Website, surreptitiously forcing Plaintiff and Class Members to transmit to Facebook every click, keystroke, and intimate detail about their medical treatment. Operating as designed and as implemented by Defendants, the Pixel allows the Private Information that Plaintiff and Class Members submit to Defendants to be unlawfully disclosed to Facebook alongside the individual's unique and persistent Facebook ID ("FID").[5]

8. A pixel is a piece of code that "tracks the people and [the] type of actions they take"[6] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), among other things.

9. The user's web browser executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Facebook Pixel is thus customizable and programmable, meaning that the website owner controls which of its webpages contain the Pixel and which events are tracked and transmitted to Facebook.

---

[5] The Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited: January 27, 2023)

[6] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Feb. 17, 2023).

10. By installing the Facebook Pixel on its Website, Defendants effectively planted a bug on Plaintiff's and Class Members' web browsers and compelled them to disclose their communications with Defendants to Facebook.

11. In addition to the Facebook Pixel, Defendants also installed and implemented Facebook's Conversions Application Programming Interface ("CAPI") on its Website servers.[7]

12. Unlike the Facebook Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.[8,9]

13. Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[10]

14. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendants to circumvent any ad blockers or other denials of consent by the website user that would prevent the Pixel from sending

---

[7] "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited: January 25, 2023).

[8] https://revealbot.com/blog/facebook-conversions-api/ (last visited: January 24, 2023).

[9] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel.... This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels.", https://developers.facebook.com/docs/marketing-api/conversions-api (last visited: January 27, 2023).

[10] https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited: January 28, 2023).

website users' Private Information to Facebook directly.

15. Defendants utilized the Pixel and CAPI data for marketing purposes in an effort to bolster its profits. The Facebook Pixel and CAPI are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiff's and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendants.

16. The information that Defendants' Tracking Pixel and CAPI sent to Facebook included the Private Information that Plaintiff and Class Members submitted to Defendants' Website, including for example, the type of medical treatment sought, the individual's particular health condition, and the fact that the individual attempted to or did book a medical appointment.

17. Such information allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers who geotarget Plaintiff's and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and CAPI. Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

18. Healthcare patients simply do not anticipate that their trusted healthcare provider will send personal health information or confidential medical information collected via its webpages to a hidden third party—let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the patients' consent.

19. Neither Plaintiff nor any other Class Member signed a written authorization permitting Defendants to send their Private Information to Facebook.

20. Despite willfully and intentionally incorporating the Facebook Pixel and CAPI into its Website and servers, Conemaugh Heath System has never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook. Plaintiff and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook as they communicated their confidential PHI with their healthcare provider via the Website, or stored on Defendants' servers to be later transmitted to Facebook so it could be used for targeted advertising and marketing purposes.

21. Defendants further made expressed and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendants.

22. Defendants owed common law, statutory, and regulatory duties to keep Plaintiff's and Class Members' communications and medical information safe, secure, and confidential.

23. Upon information and belief, Conemaugh Health System utilized the Pixel data to improve and to save costs on its marketing campaigns, improve its data analytics, and attract new patients.

24. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties to those individuals to protect and to safeguard that information from unauthorized disclosure.

25. Defendants breached their statutory and common law obligations to Plaintiff and Class Members by, *inter alia*,: (i) failing to adequately review its marketing programs and web based technology to ensure the hospital Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) aiding, agreeing, and conspiring with third-parties to intercept communications sent and received by Class

Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook or others; (v) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Facebook Pixels; (vi) failing to warn Plaintiff and Class Members; and (vii) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

26. Plaintiff seek to remedy these harms and bring causes of action for (I) Invasion of Privacy, (II) Breach of Implied Contract, (III) Unjust Enrichment; (IV) Breach of Fiduciary Duty, (V) Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. § 20101 *et. seq.*, and (VI) Violation of the Pennsylvania Wiretapping and Electronic Surveillance Control Act 18 Pa. C.S. § 5701 et seq., ("WESCA").

PARTIES

27. Plaintiff, Jane Doe is a natural person, resident, and a citizen of the Commonwealth of Pennsylvania, where she intends to remain, with a principal residence in Johnstown, Cambria County. She is a patient and former patient of Conemaugh Health System and a victim of Defendants' unauthorized disclosure of Private Information via the Meta Pixel.

28. Defendant, DLP Conemaugh Memorial Medical Center, LLC, is a Delaware limited liability company with its principal place of business in the Commonwealth of Pennsylvania at 1086 Franklin Steet, Johnstown, Pennsylvania 15905 in Cambria County, doing business as Conemaugh Health System d/b/a Conemaugh Memorial Medical Center (hereinafter "Conemaugh Health System").

29. Defendant, DLP Conemaugh Physician Practices, LLC d/b/a Conemaugh Physician Group - Ob/Gyn ("Conemaugh Physician Group - Ob/Gyn,") is a Delaware limited liability company with its principal place of business at 1111 Franklin Street, Suite 300, Johnstown,

Pennsylvania 15905 in Cambria County (collectively with Conemaugh Health System "Defendants").

JURISDICTION AND VENUE

30. This Court has jurisdiction over the subject matter of this action pursuant to 42 Pa. Cons. Stat. § 931.

31. This Court has personal jurisdiction over Defendants pursuant to 42 Pa. Cons. Stat. § 5301, because Defendants each carry on of a continuous and systematic part of their general business within this Commonwealth and maintain principal places of business herein, and further upon information and belief as each have qualified as a foreign entity under the laws of Pennsylvania.

32. Venue is appropriate in this Court under 231 Pa. Code § 2179, because Defendants' principal places of business are in Cambria County.

COMMON FACTUAL ALLEGATIONS

A. Background

33. Since 2014, Conemaugh Health System has owned and operated Conemaugh Memorial Medical Center whose headquarters and main campus are located at 1086 Franklin Street, Johnstown, Pennsylvania, 15905.

34. As described by Conemaugh Health System, Conemaugh Memorial Medical Center "is the flagship hospital of Conemaugh Health System," with over 500 beds, "[a] regional referral hospital known for clinical excellence, [and] home to the highest level of care designations for Neonatal Care (Level 3) and Trauma Care (Level 1)."[11]

35. At Conemaugh Memorial Medical Center, Conemaugh Health System, provides

[11] https://www.conemaugh.org/conemaugh-memorial-medical-center

myriad medical, surgical, and other treatment services including care relating to Bariatrics & Weight Loss, Black Lung Screening, Brain & Spine, Cancer Care, Critical Care, Diabetes Care, Emergency & Trauma, Food and Nutrition Services, General Surgery, GI & Digestive Health, Heart & Vascular, Home Health & Hospice, diagnostic imaging, infusion, radiological services, laboratory services, maternity care, orthopedics, ostomy care, palliative care, plastic surgery, pulmonary care, rehabilitation services, treatment for sleep disorders, "spiritual care," stroke care, other surgical services, a Transitional Care Unit, Trauma Services, Women's Health care, and wound care.[12]

36. Moreover, within Conemaugh Memorial Medical Center, Conemaugh Physician Group - Ob/Gyn provides obstetrics and gynecological medical treatment to patients at 1111 Franklin Street, Suite 300, Johnstown, PA 15905.

37. Collectively, Defendants serve their patients via its Online Platforms, which it encourages patients to use for finding providers, scheduling appointments and/or procedures, communicating with their healthcare providers, reviewing their medical histories and related documents, and communicating other information related to their treatment and status as a patient.

38. Notably, Defendants encourage patients and prospective patients find physicians through the "Find a Doctor" function of the Online Platforms, https://www.conemaugh.org/find-a-doctor, even as it cautions that many such healthcare providers are independent contractors and not hospital employees, representatives, or agents. This includes gynecologists who are employees and agents of Conemaugh Physician Group - Ob/Gyn.

39. Defendants promote the convenience and comprehensive functionality of its Online Platforms, allowing patients to find services and providers, schedule appointments, find medical

[12] *See Id.*

information; as well as to utilize MyChart, stating that:

> Conemaugh Health System's online Patient Portal, **Conemaugh MyChart**, is available for all Conemaugh Health System and Conemaugh Physician Group patients. This **FREE** online tool provides access to personal health records -- anywhere, anytime![13]

40. Defendants use Conemaugh Health System's Website to connect Plaintiff and Class Members to Defendants' digital healthcare platforms with the goal of increasing profitability.

41. In furtherance of that goal, and to increase the success of its advertising and marketing, Defendants purposely installed the Facebook pixel and Facebook's Conversions API tools on many of its webpages within its Website and on its servers and programmed those webpages and servers. In doing so, Defendants surreptitiously shared patients' private and protected communications with Facebook, including communications that contain Plaintiff's and Class Members' Private Information.

42. To better understand Defendants' unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows:

i. Facebook's Business Tools and the Meta Pixel

43. As Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[14]

44. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendants, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

---

[13] https://www.conemaugh.org/patient-portal

[14] Facebook, *Meta Reports Fourth Quarter and Full Year 2021 Results* , https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022).

45. Facebook's Business Tools, including the Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

46. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"), as well as metadata, button clicks, and other information.[15] Businesses that want to target customers and advertise their services, such as Defendants, can track other user actions and can create their own tracking parameters by building a "custom event."[16]

47. One such Business Tool is the Pixel that "tracks the people and type of actions they take."[17] When a user accesses a webpage that is hosting the Pixel, the communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook—traveling from the user's browser to Facebook's server.

48. Notably, this transmission only occurs on webpages that contain the Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate privacy (such as the homepage) and disable it on pages that do implicate patient privacy (such as the "find a doctor" page). Thus, Plaintiff's and Class Member's Private Information would not have been disclosed to Facebook via the Pixel but for Defendants' decisions to install the Pixel on

---

[15] Facebook, *Specifications for Facebook Pixel Standard Events*, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited Jan. 31, 2023); *see* Facebook, *Facebook Pixel, Accurate Event Tracking, Advanced*, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Facebook, *Best Practices for Facebook Pixel Setup*, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; Facebook, *App Events API*, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 31, 2023).

[16] Facebook, *About Standard and Custom Website Events*, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* Facebook, *App Events API*, *supra*.

[17] Facebook, *Retargeting*, https://www.facebook.com/business/goals/retargeting.

its Website and specifically on the webpages that solicit and receive Private Information.

49. The Meta Pixel's primary purpose is for marketing and ad targeting.[18]

50. Meta's own website informs companies that "The Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[19]

51. According to Meta, the Meta Pixel can collect the following data:

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and ***person using the website.*** (emphasis added).
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
>
> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
>
> **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[20]

52. Meta boasts to its prospective users that the Meta Pixel can be used to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.
- **Drive more sales.** Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.
- **Measure the results of your ads.** Better understand the impact of your ads

[18] *See Meta Pixel*, META FOR DEVELOPERS https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[19] *About Meta Pixel*, Meta Business Help Center. https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last accessed Mar. 19, 2023).
[20] *Meta Pixel*, META FOR DEVELOPERS https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

by measuring what happens when people see them.[21]

53. Meta/Facebook likewise benefits from the data received from the Pixel and uses the data to serve targeted ads and identify users to be included in such targeted ads.

ii. Defendants' method of transmitting Plaintiff's and Class Members' Private Information via the Tracking Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Pixel

54. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

55. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

56. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies.[22]

57. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), they also send the host server data, which is embedded inside the URL and can include cookies.

---

[21] *About Meta Pixel*, Meta Business Help Center. https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last accessed Mar. 19, 2023).

[22] "Cookies are small files of information that a web server generates and sends to a web browser. ...Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

58. When an individual visits Defendants' Website, their web browser sends an HTTP Request to Defendants' servers that essentially asks Defendants' Website to retrieve certain information (such as Defendants' "Make an Appointment" page). Defendants' servers sends the HTTP Response, which contains the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendants' Website.

59. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

60. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user, and this is exactly what happened when patients used Defendants' Website and Online Platforms.

61. Defendants' implementation of the Pixel is source code that acted much like a traditional wiretap, intercepting and transmitting communications intended only for Defendants.

62. Separate from the Pixel, Facebook and other website owners can place third-party cookies in the web browsers of users logged into their websites or services. These cookies can uniquely identify the user so the cookie owner can track the user as she moves around the internet—whether on the cookie owner's website or not. Facebook uses this type of third-party cookie when Facebook account holders use the Facebook app or website. As a result, when a Facebook account holder uses Defendants' Website, a unique id is sent to Facebook along with the intercepted communication that allows Facebook to identify the patient associated with the Private Information it has intercepted.

63. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. To counteract this, third parties bent on gathering data and Private Information implement workarounds that are difficult to detect or evade. Facebook's workaround is its Conversions API tool, which is particularly effective because the data transmitted via this tool does not rely on the website visitor's web browsers. Rather, the information travels directly from Defendants' server to Facebook's server.

64. Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]." Thus, Defendants receives and stores its communications with patients on its server before Conversions API collects and sends those communications—and the Private Information contained therein—to Facebook.

65. Notably, client devices do not have access to host servers and thus cannot prevent (or even detect) this additional transmission of information to Facebook.

66. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the host server, Facebook instructs companies like Defendants to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendants "to share website events [with Facebook] that the pixel may lose."[23] Thus, since Defendants implemented the Pixel in in accordance with Facebook's documentation, it is also reasonable to infer that Defendants implemented the Conversions API tool on its website.

67. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content on the host website. In other words, Facebook and others like it are not providing anything to the user relating to the user's communications.

[23] *See* https://www.facebook.com/business/help/308855623839366?id= 818859032317965 (last visited Jan. 23, 2023).

Instead, these third parties are typically procured to track user data and communications only to serve the marketing purposes of the website owner (*i.e.,* to bolster profits).

68. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendants can use its source code to commandeer its patients' computing devices, causing the device's web browser to contemporaneously and invisibly re-direct the patients' communications to hidden third parties like Facebook.

69. In this case, Defendants employed the Tracking Pixel and Conversions API to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook contemporaneously, invisibly, and without the patient's knowledge.

70. Consequently, when Plaintiff and Class Members visited Defendants' website and communicated their Private Information, including, but not limited to, medical treatment sought, medical conditions, appointment type and date, physician selected, specific button/menu selections, content (such as searches for symptoms or treatment options) typed into free text boxes, demographic information, email addresses, phone numbers, and emergency contact information, it is simultaneously intercepted and transmitted to Facebook.

iii. Defendants Violated Their own Privacy Policies

71. Conemaugh Health System maintains Patient Privacy Practices which apply to "***all*** Conemaugh Health System facilities and affiliates" (emphasis added).[24]

72. Defendants' Patient Privacy Practices provide, "[t]his notice describes how medical information about you may be used and disclosed and how you can get access to this information."[25]

---

[24] *See* Conemaugh Health System Patient Privacy Practices, available at https://www.conemaugh.org/sites/conemaugh/assets/uploads/Patient%20Privacy%20Practices%20rev.%202023.pdf (last accessed April 14, 2023) (attached hereto as **Exhibit A**).

[25] *Id*

73. The Patient Privacy Practices state, "**In these cases we never share your information unless you give us written permission:** • Marketing purposes. • Sale of your information…"[26]

74. Therein, Defendants further acknowledge, represents and promises:

> **Our Responsibilities**
>
> • We are required by law to maintain the privacy and security of your protected health information.
>
> • We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
>
> • We must follow the duties and privacy practices described in this notice and give you a copy of it.
>
> • We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind. For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.[27]

75. Defendants' Notice of Privacy Practices does not permit Defendants to use and disclose Plaintiff's and Class Members' Private Information for marketing purposes without written permission.[28]

76. Defendants violated their own Patient Privacy Practices by unlawfully disclosing Plaintiff's and Class Members' Private Information to Facebook, Meta, Google, and likely other third parties.

77. Further, Defendants maintain an online privacy policy ("Online Privacy Policy")[29] provides:

> This Public Online Privacy Policy and the links included explain how we collect, treat, and protect your individually identifiable personal information. Specifically, the Public Online Privacy Statement describes how we handle the personal

[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] Conemaugh Health System website "Privacy Policy," available at https://www.conemaugh.org/privacy-policy (attached hereto as **Exhibit B).**

information that you submit to us when you submit a Contact Us form, attach a resume, and browse our website.

[...]

We've designed our public websites to capture two types of information: automatic tracking and individually identifiable personal information ("personal information").

78. The Online Privacy Policy goes onto explain that:

Personal information can be anything you've provided through our public websites that identifies you. For example: Your name, email address, and street address are types of personal information. We store this information behind a complex series of firewalls, in a way that maximizes security and confidentiality.

79. Defendants' Online Privacy Policies promises that:

- We will only use the information to provide you with the services you have requested and as otherwise described in this Public Online Privacy Policy
- We will NOT sell, rent, or license the personal information you provide within our public websites.
- We do NOT provide any personally identifiable information about our users to any third party.
- Access to the data you submit is limited to the authorized staff detailed in our Site Disclaimer under Security.[30]

80. Defendants' Online Privacy Policy goes on to say:

We use "cookies" to personalize our site for you and to collect aggregate information about site usage by all of our users. A cookie is a text file that our website transfers to your computer's hard drive for record keeping purposes. The cookie assigns a random, unique number to your computer. **It does not contain information that would personally identify you.**[31]

81. Defendants unlawfully disclosed Plaintiff's and Class Members' Private Information to Facebook, Meta, and likely other third parties, without authorization, in violation its own Patient Privacy Practices and Online Privacy Policy.

[30] *Id.* (emphasis in original).
[31] *Id* (emphases added)

82. Defendants further misrepresented that they would preserve the confidentiality of their Private Information and the anonymity of their identities.

83. Despite the representations in its privacy policies, Defendants do indeed transfer PII and PHI, Private Information, to third parties. An example illustrates the point. If a user visits Defendants' website and clicks on the "Find a Doctor" tab (https://www.conemaugh.org/find-a-doctor), the individual's browser sends a request to Defendants' server requesting that it load the webpage. Because Defendants utilize the Facebook Pixel, Facebook's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, causing it to secretly duplicate the communication with Defendants, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

84. For example, if the user clicks "Find a Doctor" and enters their Zip Code and the doctor's specialty, like "Addiction Medicine," this is information is shared with Facebook, Google, or others that Defendants has configured its Pixel to interact with.

85. After collecting and intercepting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

86. Every time Defendants send a patient's website activity data to Facebook, that patient's PII is also disclosed, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to the corresponding Facebook profile and the persons real world identity. A user who accesses Defendants' digital platforms while logged into Facebook will

transmit the user cookie to Facebook, which contains that user's unencrypted Facebook ID.

87. Google and other companies likewise process this data in a similar manner and use it to connect the information to particular individuals to build marketing and other data profiles.

88. Through the Pixel, Defendants share their patients' identities and online activity, including personal information and search results related to their private medical treatment.

89. Defendants could have configured its tracking software to limit the information that it communicated to third parties, but it did not and instead intentionally selected the features and functionality of the Pixel that resulted in the Disclosure.

90. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendants to disclose their Private Information and assist with intercepting their communications. Plaintiff were never provided with any written notice that Defendants discloses its patients' protected health information, nor were they provided any means of opting out of such disclosures. Defendants nonetheless knowingly disclosed Plaintiff's protected health information to Meta, Facebook, Google, and other unauthorized entities.

91. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

92. By law, Plaintiff are entitled to privacy in his protected health information and confidential communications. Defendants deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential communications, personally identifiable information, and protected health information; (2) disclosed patients' protected information to Facebook and

others—unauthorized third-party eavesdroppers; and (3) undertook this pattern of conduct without notifying Plaintiff and Class Members and without obtaining their express written consent. Plaintiff did not discover that Defendants disclosed their personally identifiable information and protected health information to Facebook and Google, and assisted Facebook and Google with intercepting their communications.

B. Plaintiff's Experience

93. Plaintiff Jane Doe is a patient of Defendants, receiving services both at Conemaugh Health System's Conemaugh Memorial Medical Center, and within their physician's network at Conemaugh Physician Group - Ob/Gyn that relied on Defendant's digital healthcare platforms to communicate confidential patient information.

94. Plaintiff accessed Defendants' digital tools to receive healthcare services from Defendants and at Defendants' direction and encouragement, to find physicians, to find different hospital locations, to check her test results, to communicate with physicians, and confirm appointments. Plaintiff last used these digital tools on April 13, 2023, to check her test results.

95. Plaintiff reasonably expected that her online communications with Defendants were confidential, solely between herself and Defendants, and that such communications would not be transmitted to or intercepted by a third party.

96. Plaintiff provided his Private Information to Defendants and trusted that the information would be safeguarded according to Conemaugh Health System's privacy policies and state and federal law.

97. As described herein, Defendants sent Plaintiff's Private Information to Facebook, Google, and others when she used Defendants' digital platforms to communicate healthcare and identifying information to Defendants.

98. Pursuant to the process described herein, Defendants assisted Facebook, Google, and others with intercepting Plaintiff Jane Doe's communications, including those that contained PII, PHI, and related confidential information. Defendants facilitated these interceptions without Plaintiff Jane Doe's knowledge, consent, or express written authorization.

99. By failing to receive the requisite consent, Defendants breached confidentiality and unlawfully disclosed Plaintiff Jane Doe's Private Information, PII and PHI.

C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI

100. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[32] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

101. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective … at preventing the receipt of sensitive data."[33]

102. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data is not misplaced. In June 2022, the FTC finalized a

[32] https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/
[33] https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf

different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[34] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[35]

103. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[36]

104. Furthermore, in June 2022, an investigation by The Markup[37] revealed that the Meta Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[38] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by

[34] https://slate.com/technology/2022/06/health-data-brokers-privacy.html
[35] https://slate.com/technology/2022/06/health-data-brokers-privacy.html
[36] https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes
[37] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* www.themarkup.org/about (last accessed Mar. 19, 2023).
[38] PIXEL HUNT, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last accessed Mar. 19, 2023).

clicking a button to schedule a doctor's appointment.[39] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[40]

105. The Markup article found during the course of its investigation that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[41]

106. Despite knowing that the Meta Pixel code embedded in its websites was sending patients' personal health information, Private Information, to Facebook, Defendants did nothing to protect its patients from egregious intrusions into its patients' privacy, choosing instead to benefit at those patients' expense.

107. In addition to the 33 hospitals identified by The Markup that had installed the Meta Pixel on their websites, The Markup identified seven health systems that had installed the pixels inside their password-protected patient portals.[42]

108. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply troubled" by what the hospitals were doing by capturing patient data and sharing it.[43]

---

[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*

D. Defendants Violated HIPAA Standards

109. Under Pennsylvania law and HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[44]

110. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

111. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[45]

112. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).[46]

---

[44] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
[45] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 3, 2022).
[46] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Nov. 3, 2022)

113. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[47]

114. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[48]

115. Citing The Markup's June 2022 article, the Bulletin expressly notes:

> Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
>
> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule.[49]

116. In other words, HHS has expressly stated that Defendants' conduct of

---

[47] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.
[48] *Id.*
[49] *Id.* (emphasis in original) (internal citations omitted).

implementing the Facebook Pixel is a violation of HIPAA Rules.

E. Defendants Violated Industry Standards

117. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

118. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications, which are applicable to Defendants, and their physicians.

119. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy).

120. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

121. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must…:(c) release patient information only in keeping ethics guidelines for confidentiality.

F. Plaintiff's and Class Members' Expectation of Privacy

122. Plaintiff and Class Members were aware of Defendants' duty of confidentiality when they sought medical services from Defendants.

123. Indeed, at all times when Plaintiff and Class Members provided their Private Information to Defendants, they all had a reasonable expectation that the information would remain private and that Defendants would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

G. IP Addresses are Personally Identifiable Information

124. On information and belief, through the use of the Facebook Pixel on Defendants' Website, Defendants also disclosed and otherwise assisted Facebook with intercepting Plaintiff's and Class Members' Computer IP addresses.

125. An IP address is a number that identifies the address of a device connected to the Internet.

126. IP addresses are used to identify and route communications on the Internet.

127. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

128. Facebook tracks every IP address ever associated with a Facebook user.

129. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

130. Under HIPAA, an IP address is considered personally identifiable information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. See 45 C.F.R. § 164.514 (2).

- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

131. Consequently, by disclosing IP addresses, Defendants' business practices violated

HIPAA and industry privacy standards.

H. Defendants Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures

132. The sole purpose of the use of the Facebook Pixel on Defendants' Website was marketing and profits.

133. In exchange for disclosing the Private Information of its patients, Defendants is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on its platform.

134. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendants re-targeted patients and potential patients.

135. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendants.

I. Plaintiff's and Class Members' Private Information Had Financial Value

136. Plaintiff's data and Private Information has economic value. Facebook regularly uses data that it acquires to create Core and Custom Audiences, as well as Lookalike Audiences and then sells that information to advertising clients.

137. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to increase; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

138. The value of health data in particular is well-known, and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How

Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[50]

139. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[51]

CLASS ALLEGATIONS

140. Plaintiff brings this statewide class action on behalf of herself and on behalf of other similarly situated persons.

141. The Statewide Class that Plaintiff seeks to represent is defined as follows:

> **All Pennsylvania citizens whose Private Information was disclosed by Defendants to third parties through the Meta Pixel and related technology without authorization.**

142. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

143. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

---

[50] *See* https://time.com/4588104/medical-data-industry/ (last visited February 16, 2023).
[51] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited February 16, 2023).

144. **Numerosity:** Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly accessed in the Disclosure, and each Class is apparently identifiable within Defendants' records.

145. **Commonality:** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect Plaintiff's and Class Members' Private Information;

b. Whether Defendants had duties not to disclose the Plaintiff's and Class Members' Private Information to unauthorized third parties;

c. Whether Defendants had duties not to use Plaintiff's and Class Members' Private Information for non-healthcare purposes;

d. Whether Defendants had duties not to use Plaintiff's and Class Members' Private Information for unauthorized purposes;

e. Whether Defendants failed to adequately safeguard Plaintiff's and Class Members' Private Information;

f. Whether and when Defendants actually learned of the Disclosure;

g. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

h. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

i. Whether Defendants failed to properly implement and configure the tracking software on its digital platforms to prevent the disclosure of information

compromised in the Disclosure;

j. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Disclosure to occur;

k. Whether Defendants engaged in unfair, unlawful, or deceptive practices by misrepresenting that it would safeguard Plaintiff's and Class Members' Private Information;

146. **Typicality:** Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Disclosure, due to Defendants' use and incorporation of the tracking software.

147. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendants has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

148. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff have suffered are typical of other Class Members. Plaintiff have also retained counsel experienced in complex class action litigation, and Plaintiff intend to prosecute this action vigorously.

149. **Superiority and Manageability:** Class litigation is an appropriate method for fair

and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

150. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

151. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

152. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

153. Unless a Class-wide injunction is issued, Defendants may continue in its unlawful disclosure and failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Disclosure, and Defendants may continue to act unlawfully as set forth in this Complaint.

154. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

155. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. Whether an implied contract existed between Defendants on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied

contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Disclosure;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

156. Plaintiff realleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

157. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendants, Conemaugh Health System and Conemaugh Physician Group - Ob/Gyn

158. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendants via their website and the communications platforms and services therein.

159. Plaintiff and Class Members communicated sensitive PHI and PII that they

intended for only Defendants to receive and that they understood Defendants would keep private.

160. Defendants' disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and Class Members is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion.

161. Plaintiff and Class Members had a reasonable expectation of privacy given Defendants' representations, Notice of Privacy Practices, Terms of Use, and HIPAA. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential. Defendants' disclosure of PHI coupled with PII is highly offensive to the reasonable person.

162. As a result of Defendants' actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

163. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages.

164. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

165. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendants' actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendants from engaging in such conduct in the future.

166. Plaintiff also seek such other relief as the Court may deem just and proper.

COUNT II
BREACH OF IMPLIED CONTRACT

(On behalf of Plaintiff and the Class)

167. Plaintiff realleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

168. Defendants required Plaintiff and the Class Members to provide their Private Information, including full names, email addresses, phone numbers, computer IP addresses, appointment information, medical insurance information, medical provider information, medical histories, and other content submitted on Defendants' website and billing portal as a condition of their receiving healthcare services.

169. As a condition of utilizing Defendants' digital platforms and receiving services from Defendants, Plaintiff and the Class provided their Private Information and compensation for their medical care. In so doing, Plaintiff and the Class entered into contracts with Defendants by which Defendants agreed to safeguard and protect such information, in its Privacy Practices and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

170. Implicit in the agreement between Defendants and their patients was the obligation that both parties would maintain the Private Information confidentially and securely.

171. Defendants had an implied duty of good faith to ensure that the Private Information of Plaintiff and Class Members in its possession was only used only as authorized, such as to provide medical treatment, billing, and other medical benefits from Conemaugh Health System and Conemaugh Physician Group - Ob/Gyn.

172. Defendants had an implied duty to protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses.

173. Additionally, Conemaugh Health System and Conemaugh Physician Group -

Ob/Gyn implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

174. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendants, Conemaugh Health System and Conemaugh Physician Group - Ob/Gyn. Defendants did not. Plaintiff and Class Members would not have provided their confidential Private Information to Defendants in the absence of their implied contracts with Defendants and would have instead retained the opportunity to control their Private Information for uses other than medical treatment, billing, and benefits from Conemaugh Health System and Conemaugh Physician Group - Ob/Gyn.

175. Defendants breached the implied contracts with Plaintiff and Class members by disclosing Plaintiff's and Class Members' Private Information to an unauthorized third party.

176. Defendants' acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiff and Class Members to provide their Private Information in exchange for medical treatment and benefits.

177. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiff and the Class have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities.

178. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

179. Plaintiff realleges and incorporate the preceding paragraphs of this Complaint as if fully set forth herein.

180. This claim is pleaded solely in the alternative to Count II.

181. Plaintiff and Class members conferred a monetary benefit upon Defendants, Conemaugh Health System and Conemaugh Physician Group - Ob/Gyn in the form of valuable sensitive medical information that Defendants collected from Plaintiff and Class Members under the guise of keeping this information private. Defendants collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiff and the Class Members conferred a benefit on Defendants in the form of monetary compensation.

182. Plaintiff and Class Members would not have used Defendants' services or would have paid less for those services, if they had known that Defendants would collect, use, and disclose this information to third parties.

183. Defendants appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class members.

184. As a result of Conemaugh Health System's and Conemaugh Physician Group - Ob/Gyn's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

185. The benefits that Defendants derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles for Defendants to be permitted to retain any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

186. Defendants should be compelled to disgorge into a common fund for the benefit

of Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of its conduct and the Disclosure alleged herein.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

187. Plaintiff realleges and incorporate the preceding paragraphs of this Complaint as if fully set forth herein.

188. A relationship existed between Plaintiff and the Class on the one hand and Defendants on the other in which Plaintiff and the Class put their trust in Defendants, Conemaugh Health System and Conemaugh Physician Group - Ob/Gyn, to protect the Private Information of Plaintiff and the Class and Defendants accepted that trust.

189. Defendants breached the fiduciary duty that it owed to Plaintiff and the Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect, and intentionally disclosing, the Private Information of Plaintiff and the Class.

190. Defendants' breach of fiduciary duty was a legal cause of damage to Plaintiff and the Class.

191. But-for Defendants' breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred.

192. Defendants' breach of fiduciary duty contributed substantially to producing the damage to the Plaintiff and the Class.

193. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiff and Class Members are entitled to and do demand actual, consequential, and nominal damages,

injunctive relief, and all other relief allowed by law.

COUNT V
VIOLATION OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 PA. STAT. § 20101 *ET. SEQ.* ("UTPCPL")
(On Behalf of Plaintiff and the Class)

194. Plaintiff realleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

195. Plaintiff, the members of the Class, and Defendant are all "persons" within the meaning of the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), 73 Pa. Stat. § 201-2(2).

196. The UTPCPL prohibits "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."

197. Under the UTPCPL, "[u]nfair or deceptive acts or practices" include: "[r]epresenting that… services have sponsorship, approval, characteristics, . . . [or] benefits . . . that they do not have," 73 Pa. § 201-2(4)(v); "[r]epresenting that… services are of a particular standard . . . [or] quality . . . if they are of another," *id.* § 201-2(4)(vii); "[a]dvertising… services with intent not to sell them as advertised," *id.* § 201-2(4)(ix); and "[e]ngaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding," *id.* § 201-2(4)(xxi).

198. Defendants' acts, practices, and omissions alleged in this Complaint constitute unlawful, unfair, and deceptive acts and practices under the UTPCPL.

199. Defendants knew or should have known about the unauthorized disclosure of

Plaintiff's and the Class's Private Information via the Meta Pixel, yet Defendants concealed that information from Plaintiff and the Class.

200. Defendants engaged in unlawful, unfair, and deceptive acts and practices prohibited by the UTPCPL by, among other things: misrepresenting or omitting material facts to Plaintiff and the Class regarding the adequacy of Defendants' protection of their Private Information, in violation of 73 Pa. Stat. §§ 201-(4)(v), (vii), (ix), and (xxi);

201. Defendants' acts and omissions and its misrepresentations were intentional, knowing, and undertaken to mislead the public, including Plaintiff and the members of the Class.

202. Defendants' unlawful, unfair, and deceptive acts and practices were unethical, oppressive, and unscrupulous. These acts and practices caused substantial injury to Plaintiff and members of the Class that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

203. Defendants possessed exclusive knowledge about the disclosure of Plaintiff's and the Class Member's Private Information to unauthorized parties via the Meta Pixel to their detriment.

204. Defendants had a duty to disclose the foregoing to Plaintiff and members of the Class, and failed to do so.

205. Plaintiff and members of the Class reasonably relied on Defendants to protect and safeguard their Private Information and to promptly and adequately inform them of the unauthorized Disclosure.

206. Defendants owed Plaintiff and the Class a duty to: maintain the privacy and security of Plaintiff's and the Class's Private Information; take proper action to prevent the Disclosure; take

proper action following the Disclosure to protect further unauthorized disclosure, release, and theft of Private Information, and promptly inform Plaintiff and members of the Class about the breach.

207. Plaintiff and members of the Class suffered ascertainable losses of money or property as a result of Defendants' use and employment of methods, acts, or practices declared to be unlawful by 73 Pa. §§ 201-2(2) and 201-(3).

208. Plaintiff and the Class seek an order enjoining Defendants' unlawful acts and practices and awarding any other just and proper relief available under the UTPCPL including actual or statutory damages, treble damages, and attorneys' fees and costs.

COUNT VI
VIOLATION OF THE PENNSYLVANIA WIRETAPPING AND ELECTRONIC SURVEILLANCE CONTROL ACT 18 PA. C.S. § 5701, *ET SEQ.* ("WESCA")
(On Behalf of Plaintiff and the Class)

209. Plaintiff realleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

210. WESCA defines "Person" as any employee, or agent of the United States or any state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust or corporation. 18 Pa. C.S.A. § 5702.

211. Defendants each constitute a "person" under WESCA, 18 Pa. C.S.A. § 5702.

212. The Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S.A. §§ 5701, 5703(1) ("WESCA") prohibits any person from willfully intercepting, endeavoring to intercept, or procuring of any other person to intercept or endeavor to intercept, any wire, electronic, or oral communication.

213. WESCA, 18 Pa. C.S.A. § 5702 defines "intercept," as "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. C.S.A. § 5702.

214. WESCA, 18 Pa. C.S.A. § 5703(2)-(3) also prohibits the disclosure of, or use of, the contents of any wire, electronic, or oral communication, or any evidence derived therefrom, with knowledge that the information was obtained through the interception of a wire, electronic, or oral communication.

215. WESCA, 18 Pa. C.S.A. § 5741(a) further prohibits the knowing access without authorization of a facility through which an electronic communication is provided or exceeds an authorization to access that facility and obtains, or alters access to a wire or electronic communication while that communication is in electronic storage.

216. WESCA, 18 Pa. C.S.A. § 5741, is also violated where, for the purpose of commercial advantage or private commercial gain, a person knowingly accesses without authorization a facility through which an electronic communication service is provided, or exceed access to that facility, and obtains access to a wire or electronic communication while that communication is in electronic storage.

217. As set forth herein, Defendants knowingly, willfully, and intentionally intercepted and disclosed Plaintiffs' and Class Members' electronic communications, without the consent of the Plaintiffs and Class Members, using Facebook's tracking devices.

218. Defendants knowingly, willfully, and intentionally intercepted Plaintiffs' and Class Members' electronic communications for the purpose of disclosing those communications to third parties including Facebook without the knowledge, consent, or written authorization of Plaintiffs or Class Members.

219. The devices used in this case, include, but are not limited to:

a. to which Plaintiffs' and Class Members' communications were disclosed.

b. Plaintiffs' and Class Members' personal computing devices;

c. Plaintiffs' and Class Members' web browsers;

d. Plaintiffs' and Class Members' browser-managed files;

e. Facebook's Pixel;

f. Internet cookies;

g. Defendant's computer servers;

h. Third-party source code utilized by Defendant; and

i. Computer servers of third parties (including Facebook)

220. Defendants aided in the interception of communications between Plaintiffs and Class Members and Defendant that were redirected to and recorded by third parties without the Plaintiffs or Class Members consent.

221. WESCA confers a private civil cause of action to any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation thereof against "any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. C.S. § 5725(a).

222. As a result of Defendants violations of WESCA, pursuant to 18 Pa. C.S.A. § 5725(a), Plaintiff and the Class Members are entitled to recover actual damages that are not less than liquidated damages computed at a rate of $100.00 a day for each day of violation or $1,000.00, whichever is higher; punitive damages; and reasonable attorneys' fees and other litigation costs reasonably incurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, JANE DOE, Individually, and on behalf of all others similarly situated, pray for judgment as follows:

A. For an Order certifying this action as a Class action and appointing Plaintiff as Class

Representatives and Plaintiff's counsel as Class Counsel;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Sensitive Information compromised during the Disclosure;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

E. Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law, including pursuant to the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. § 20101, *et seq.* ("UTPCPL"), and the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S.A. §§ 5701, *et seq.* ("WESCA");

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees under the UTPCPL, WESCA, the common fund doctrine, and any other applicable law;

I. Costs and any other expense, including expert witness fees incurred by Plaintiff

in connection with this action;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Trial by jury on all issues so triable; and,

L. Such other and further relief as this court may deem just and proper.

Dated: May 4, 2023

Respectfully submitted,

SALTZ MONGELUZZI & BENDESKY P.C.

By: Elizabeth Bailey

Elizabeth A. Bailey (Identification No. 316689)
SALTZ MONGELUZZI & BENDESKY P.C.
52nd Floor
1650 Market Street
Philadelphia, Pennsylvania 19103
(215) 496-8282
ebailey@smbb.com

Lynn A. Toops (*Pro Hac Vice* forthcoming)
Amina A. Thomas (*Pro Hac Vice* forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)

Raina C. Borelli (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class

EXHIBIT A

Conemaugh Health System

Your Information. Your Rights. Our Responsibilities

This notice describes how medical information about you may be used and disclosed and how you can get access to this information.
This notice applies to all Conemaugh Health System facilities and affiliates.

Your Rights

You have the right to:
- Get a copy of your paper or electronic medical record
- Correct your paper or electronic medical record
- Request confidential communication
- Ask us to limit the information we share
- Get a list of those with whom we've shared your information
- Get a copy of this privacy notice
- Choose someone to act for you
- File a complaint if you believe your privacy rights have been violated

Your Choices

You have some choices in the way that we use and share information as we:
- Tell family and friends about your condition
- Provide disaster relief
- Include you in a hospital directory
- Provide mental health care
- Market our services and sell your information
- Raise funds

Our Uses and Disclosures

We may use and share your information as we:
- Treat you
- Run our organization
- Bill for your services
- Help with public health and safety issues
- Do research
- Comply with the law
- Respond to organ and tissue donation requests
- Work with a medical examiner or funeral director
- Address workers' compensation, law enforcement, and other government requests
- Respond to lawsuits and legal actions

Your Rights

When it comes to your health information, you have certain rights. This section explains your rights and some of our responsibilities to help you.

Get an electronic or paper copy of your medical record
- You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this.
- We will provide a copy or a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost-based fee.

Ask us to correct your medical record
- You can ask us to correct health information about you that you think is incorrect or incomplete. Ask us how to do this.
- We may say "no" to your request, but we'll tell you why in writing within 60 days.

Request confidential communications
- You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.
- We will say "yes" to all reasonable requests.

Ask us to limit what we use or share
- You can ask us not to use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request, and we may say "no" if it would affect your care.
- If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. We will say "yes" unless a law requires us to share that information.

Get a list of those with whom we've shared information
- You can ask for a list (accounting) of the times we've shared your health information for six years prior to the date you ask, who we shared it with, and why.
- We will include all the disclosures except for those about treatment, payment, and health care operations, and certain other disclosures (such as any you asked us to make). We'll provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.

Get a copy of this privacy notice
You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.

Choose someone to act for you
- If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.
- We will make sure the person has this authority and can act for you before we take any action.

File a complaint if you feel your rights are violated
- You can complain if you feel we have violated your rights by contacting us using the information on page 1.
- You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting www.hhs.gov/ocr/privacy/hipaa/complaints/.
- We will not retaliate against you for filing a complaint.

Your Choices

For certain health information, you can tell us your choices about what we share. If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

In these cases, you have both the right and choice to tell us to:
- Share information with your family, close friends, or others involved in your care
- Share information in a disaster relief situation
- Include your information in a hospital directory

If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.

In these cases we never share your information unless you give us written permission:
- Marketing purposes
- Sale of your information
- Most sharing of psychotherapy notes

In the case of fundraising:
- We may contact you for fundraising efforts, but you can tell us not to contact you again.

Our Uses and Disclosures

How do we typically use or share your health information?
We typically use or share your health information in the following ways.

Treat you
We can use your health information and share it with other professionals who are treating you.
Example: A doctor treating you for an injury asks another doctor about your overall health condition.

Run our organization
We can use and share your health information to run our practice, improve your care, and contact you when necessary.
Example: We use health information about you to manage your treatment and services.

Bill for your services
We can use and share your health information to bill and get payment from health plans or other entities.
Example: We give information about you to your health insurance plan so it will pay for your services.

How else can we use or share your health information?
We are allowed or required to share your information in other ways – usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes.
For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.

Help with public health and safety issues
We can share health information about you for certain situations such as:
- Preventing disease
- Helping with product recalls
- Reporting adverse reactions to medications
- Reporting suspected abuse, neglect, or domestic violence
- Preventing or reducing a serious threat to anyone's health or safety

Do research
We can use or share your information for health research.

Comply with the law
We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we're complying with federal privacy law.

Respond to organ and tissue donation requests
We can share health information about you with organ procurement organizations.

Work with a medical examiner or funeral director
We can share health information with a coroner, medical examiner, or funeral director when an individual dies.

Address workers' compensation, law enforcement, and other government requests we can use or share health information about you:
- For workers' compensation claims
- For law enforcement purposes or with a law enforcement official
- With health oversight agencies for activities authorized by law
- For special government functions such as military, national security, and presidential protective services

Respond to lawsuits and legal actions
We can share health information about you in response to a court or administrative order, or in response to a subpoena.

Our Responsibilities

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.

Changes to the Terms of this Notice
We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request, in our office, and on our web site.

Conemaugh Health System's online Patient Portal, **Conemaugh MyChart**, is available for all Conemaugh Health System and Conemaugh Physician Group patients. This FREE online tool provides access to personal health records anywhere, anytime! Register at conemaugh.org/MyChart.

Conemaugh Health System Privacy Officer
814.410.8421

Making Communities Healthier

Conemaugh Health System
Duke LifePoint Healthcare

Original Notice date – April 2003 • Revised August 2010 • Revised May 2013. • Revised August 2013 • Revised April 2018 • January 2023

EXHIBIT B

Privacy Policy

Your privacy is important to us.

This Public Online Privacy Policy and the links included explain how we collect, treat, and protect your individually identifiable personal information. Specifically, the Public Online Privacy Statement describes how we handle the personal information that you submit to us when you submit a Contact Us form, attach a resume, and browse our website.

1. Information we collect:

We've designed our public websites to capture two types of information: automatic tracking and individually identifiable personal information ("personal information"). The first allows us to see which topics interest you most; the second helps us provide the services you requested.

- Automatic tracking information is gathered by following your "footsteps" online. Most web browsers automatically provide this information to the sites they visit and display. This information is not personally identifiable. We do not collect any additional data from your computer, and we do not compare data provided by your browser with any other data we maintain. The routes you—and other visitors—choose helps us learn about the people who visit our sites. We use aggregate numbers to compile statistics, monitor trends and track site usage. We also use the information to make sure our technology is compatible with yours. We're then better able to offer content, products and services that match your needs.
- Personal information can be anything you've provided through our public websites that identifies you. For example: Your name, email address, and

street address are types of personal information. We store this information behind a complex series of firewalls, in a way that maximizes security and confidentiality.

2. Information we collect:

- We will only use the information to provide you with the services you have requested and as otherwise described in this Public Online Privacy Policy
- We will NOT sell, rent, or license the personal information you provide within our public websites.
- We do NOT provide any personally identifiable information about our users to any third party.
- Access to the data you submit is limited to the authorized staff detailed in our Site Disclaimer under Security.

3. Use of cookies:

We use "cookies" to personalize our site for you and to collect aggregate information about site usage by all of our users. A cookie is a text file that our website transfers to your computer's hard drive for record keeping purposes. The cookie assigns a random, unique number to your computer. It does not contain information that would personally identify you.

SALTZ MONGELUZZI BENDESKY
TRIAL LAWYERS

DELAWARE COUNTY OFFICE
20 WEST THIRD STREET
P.O. BOX 1670
MEDIA, PA 19063
VOICE 610.627.9777
FAX 610.627.9787

ONE LIBERTY PLACE, 52ND FLOOR
1650 MARKET STREET
PHILADELPHIA, PA 19103
VOICE 215.496.8282
FAX 215.496.0999

NEW JERSEY OFFICE
8000 SAGEMORE DRIVE
SUITE 8303
MARLTON, NJ 08053
VOICE 856.751.8383
FAX 856.751.0868

LAURA MORALES, PARALEGAL
DIRECT DIAL (215) 575-2948
LMORALES@SMBB.COM

MONTGOMERY COUNTY OFFICE
120 GIBRALTAR RD
SUITE 218
HORSHAM, PA 19044
VOICE 215.496.8282
FAX 215.754.4443

May 4, 2023

VIA FEDEX DELIVERY

Cambria County Court
Of Common Pleas
200 S Center St.
Ebensburg, PA 15931

Re: Jane Doe v. DLP Conemaugh Memorial Medical Center LLC, et al.

Dear Sir/Madam:

In connection with the above matter, enclosed please find an original and one copy of Plaintiff's Amended Class Action Complaint and Jury Demand. Kindly file the original and send the time-stamped copy back to our office via the self-addressed, stamped envelope provided.

Should you have any questions, please do not hesitate to contact me.

Thank you for your assistance with this matter.

SALTZ, MONGELUZZI & BENDESKY, P.C.

/s/ Laura Morales
LAURA MORALES
Paralegal to Elizabeth A. Bailey, Esquire

lnm
Enclosures

SHERIFF'S OFFICE OF CAMBRIA COUNTY

Donald W. Robertson
Sheriff

Suzann M. Lehmier
Solicitor

JANE DOE vs. DLP CONEMAUGH MEMORIAL MEDICAL CENTER LLC D/B/A CONEMAUGH HEALTH SYSTEM D/B/A CONEMAUGH MEMORIAL MEDICAL CENTER (et al.)	**Case Number** 2023-1430

SHERIFF'S RETURN OF SERVICE

05/03/2023 01:57 PM - DEPUTY BOYD SHERRY, BEING DULY SWORN ACCORDING TO LAW, SERVED THE REQUESTED COMPLAINT IN CIVIL ACTION (CICA) BY HANDING A TRUE COPY TO A PERSON REPRESENTING THEMSELVES TO BE TRISHA ZIERER, ADMIN OFFICE CORD., WHO ACCEPTED AS "ADULT PERSON IN CHARGE" FOR DLP CONEMAUGH PHYSICIAN PRACTICES, LLC D/B/A CONEMAUGH PHYSICIANS GROUP OB/GYN AT 1111 FRANKLIN STREET, STE 300, JOHNSTOWN, PA 15901.

05/12/2023 02:55 PM - DEPUTY JEFF VIVIAN, BEING DULY SWORN ACCORDING TO LAW, STATES HE MADE DILIGENT SEARCH AND INQUIRY FOR THE WITHIN NAMED DEFENDANT TO WIT: DLP CONEMAUGH MEMORIAL MEDICAL CENTER LLC D/B/A CONEMAUGH HEALTH SYSTEM D/B/A CONEMAUGH MEMORIAL MEDICAL CENTER, BUT WAS UNABLE TO LOCATE THE DEFENDANT IN HIS BAILIWICK. THE SHERIFF THEREFORE RETURNS THE WITHIN REQUESTED COMPLAINT IN CIVIL ACTION (CICA) AS "NOT FOUND" AT 1086 FRANKLIN STREET, JOHNSTOWN, PA 15905. Office manager was not available to serve

05/17/2023 10:00 AM - DEPUTY BOYD SHERRY, BEING DULY SWORN ACCORDING TO LAW, SERVED THE REQUESTED COMPLAINT IN CIVIL ACTION (CICA) BY HANDING A TRUE COPY TO A PERSON REPRESENTING THEMSELVES TO BE MARCY DUFFY-DUKERY, OFFICE MANAGER, WHO ACCEPTED AS "ADULT PERSON IN CHARGE" FOR DLP CONEMAUGH MEMORIAL MEDICAL CENTER LLC D/B/A CONEMAUGH HEALTH SYSTEM D/B/A CONEMAUGH MEMORIAL MEDICAL CENTER AT 1086 FRANKLIN STREET, JOHNSTOWN, PA 15905.

SHERIFF COST: $163.25

SO ANSWERS,

May 17, 2023

DONALD W. ROBERTSON, SHERIFF

PROTHONOTARY OF CAMBRIA COUNTY

Lisa Crynock
Prothonotary

Bernadette Sheehan
Chief Deputy

JANE DOE
vs.
DLP CONEMAUGH MEMORIAL MEDICAL CENTER LLC (et al.)

Case Number
2023-1430

Case Participants

Plaintiff
JANE DOE

Defendant

CONEMAUGH PHYSICIAN GROUP OBGYN	1111 FRANKLIN STREET SUITE 300 JOHNSTOWN, PA15905
DLP CONEMAUGH MEMORIAL MEDICAL CENTER LLC	1086 FRANKLIN STREET JOHNSTOWN, PA15905
CONEMAUGH HEALTH SYSTEM	1086 FRANKLN STREET JOHSNTOWN, PA15905
DLP CONEMAUGH PHYSICIAN PRACTICES LLC	1111 FRANKLIN STREET SUITE 130 JOHNSTOWN, PA15905
CONEMAUGH MEMORIAL MEDICAL CENTER	1086 FRANKLIN STREET JOHNSTOWN, PA15905

Attorney (Plaintiff)

ELIZABETH A BAILEY, ESQ	1650 MARKET STREET 52ND FLOOR PHILADELPHIA, PA19103

Attorney Relationships

Plaintiff Attorney	Plaintiff
ELIZABETH A BAILEY, ESQ	JANE DOE

PROTHONOTARY DOCKET ENTRIES

Entry Date	Description	Pages

04/18/2023	CLASS ACTION COMPLAINT AND JURY DEMAND AND NOTICE FILED BY ELIZABETH A BAILEY, ESQ. {0} COPY(S) ISSUED TO THE SHERIFF, 1 COPY TO ELIZABETH A BAILEY, ESQ.	58
05/08/2023	AMENDED CLASS ACTION COMPLAINT AND JURY DEMAND FILED BY ELIZABETH BAILEY ESQ	56
05/19/2023	SHERIFF'S RETURN RECEIVED. ETC (SEE PAPER)	1
	Total Number of Pages	115

June 01, 2023